Guía de referencia

AWS Política gestionada

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Política gestionada: Guía de referencia

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué son las políticas AWS gestionadas? 1
Descripción de las páginas de referencia de las políticas 1
Políticas AWS gestionadas en desuso 2
AWS políticas gestionadas 3
AccessAnalyzerServiceRolePolicy 49
Uso de la política 49
Información de la política 49
Versión de la política 49
Documento de política JSON 50
Más información 52
AdministratorAccess 52
Uso de la política 53
Información de la política 53
Versión de la política 53
Documento de política JSON 53
Más información 53
AdministratorAccess-Amplify 54
Uso de la política 54
Información de la política 54
Versión de la política 54
Documento de política JSON 54
Más información 65
AdministratorAccess-AWSElasticBeanstalk 65
Uso de la política 65
Información de la política 65
Versión de la política 65
Documento de política JSON 66
Más información 74
AIOpsAssistantPolicy 74
Uso de la política 74
Información de la política 74
Versión de la política 75
Documento de política JSON 75
Más información 95

AIOpsConsoleAdminPolicy 95
Uso de la política 95
Información de la política 95
Versión de la política 96
Documento de política JSON 96
Más información 102
AIOpsOperatorAccess 102
Uso de la política 102
Información de la política 102
Versión de la política 102
Documento de política JSON 103
Más información 105
AIOpsReadOnlyAccess 105
Uso de la política 106
Información de la política 106
Versión de la política 106
Documento de política JSON 106
Más información 107
AlexaForBusinessDeviceSetup 107
Uso de la política 107
Información de la política 107
Versión de la política 107
Documento de política JSON 108
Más información 108
AlexaForBusinessFullAccess 109
Uso de la política 109
Información de la política 109
Versión de la política 109
Documento de política JSON 109
Más información 111
AlexaForBusinessGatewayExecution 111
Uso de la política 111
Información de la política 111
Versión de la política 111
Documento de política JSON 111
Más información 112

AlexaForBusinessLifesizeDelegatedAccessPolicy 113
Uso de la política 113
Información de la política 113
Versión de la política 113
Documento de política JSON 113
Más información 116
AlexaForBusinessNetworkProfileServicePolicy 116
Uso de la política 116
Información de la política 116
Versión de la política 116
Documento de política JSON 117
Más información 117
AlexaForBusinessPolyDelegatedAccessPolicy 117
Uso de la política 118
Información de la política 118
Versión de la política 118
Documento de política JSON 118
Más información 120
AlexaForBusinessReadOnlyAccess 120
Uso de la política 120
Información de la política 120
Versión de la política 121
Documento de política JSON 121
Más información 121
AmazonAPIGatewayAdministrator 121
Uso de la política 122
Información de la política 122
Versión de la política 122
Documento de política JSON 122
Más información 123
AmazonAPIGatewayInvokeFullAccess 123
Uso de la política 123
Información de la política 123
Versión de la política 123
Documento de política JSON 123
Más información 124

AmazonAPIGatewayPushToCloudWatchLogs 124
Uso de la política 124
Información de la política 124
Versión de la política 125
Documento de política JSON 125
Más información 125
AmazonAppFlowFullAccess 126
Uso de la política 126
Información de la política 126
Versión de la política 126
Documento de política JSON 126
Más información 129
AmazonAppFlowReadOnlyAccess 129
Uso de la política 129
Información de la política 130
Versión de la política 130
Documento de política JSON 130
Más información 131
AmazonAppStreamFullAccess 131
Uso de la política 131
Información de la política 131
Versión de la política 131
Documento de política JSON 132
Más información 133
AmazonAppStreamPCAAccess 134
Uso de la política 134
Información de la política 134
Versión de la política 134
Documento de política JSON 134
Más información 135
AmazonAppStreamReadOnlyAccess 135
Uso de la política 135
Información de la política 135
Versión de la política 136
Documento de política JSON 136
Más información 136

AmazonAppStreamServiceAccess 136
Uso de la política 137
Información de la política 137
Versión de la política 137
Documento de política JSON 137
Más información 138
AmazonAthenaFullAccess 139
Uso de la política 139
Información de la política 139
Versión de la política 139
Documento de política JSON 139
Más información 143
AmazonAugmentedAIFullAccess 143
Uso de la política 143
Información de la política 143
Versión de la política 143
Documento de política JSON 144
Más información 145
AmazonAugmentedAIHumanLoopFullAccess 145
Uso de la política 145
Información de la política 145
Versión de la política 145
Documento de política JSON 146
Más información 146
AmazonAugmentedAIIntegratedAPIAccess 146
Uso de la política 146
Información de la política 147
Versión de la política 147
Documento de política JSON 147
Más información 148
AmazonAuroraDSQLConsoleFullAccess 149
Uso de la política 149
Información de la política 149
Versión de la política 149
Documento de política JSON 149
Más información 151

AmazonAuroraDSQLFullAccess 151
Uso de la política 152
Información de la política 152
Versión de la política 152
Documento de política JSON 152
Más información 154
AmazonAuroraDSQLReadOnlyAccess 154
Uso de la política 155
Información de la política 155
Versión de la política 155
Documento de política JSON 155
Más información 156
AmazonBedrockFullAccess 156
Uso de la política 156
Información de la política 156
Versión de la política 157
Documento de política JSON 157
Más información 162
AmazonBedrockLimitedAccess 162
Uso de la política 162
Información de la política 162
Versión de la política 162
Documento de política JSON 163
Más información 165
AmazonBedrockMarketplaceAccess 165
Uso de la política 165
Información de la política 165
Versión de la política 165
Documento de política JSON 166
Más información 170
AmazonBedrockReadOnly 170
Uso de la política 170
Información de la política 170
Versión de la política 171
Documento de política JSON 171
Más información 172

AmazonBedrockStudioPermissionsBoundary 172
Uso de la política 173
Información de la política 173
Versión de la política 173
Documento de política JSON 173
Más información 177
AmazonBraketFullAccess 177
Uso de la política 178
Información de la política 178
Versión de la política 178
Documento de política JSON 178
Más información 182
AmazonBraketJobsExecutionPolicy 183
Uso de la política 183
Información de la política 183
Versión de la política 183
Documento de política JSON 183
Más información 186
AmazonBraketServiceRolePolicy 186
Uso de la política 186
Información de la política 186
Versión de la política 186
Documento de política JSON 187
Más información 187
AmazonChimeFullAccess 188
Uso de la política 188
Información de la política 188
Versión de la política 188
Documento de política JSON 188
Más información 190
AmazonChimeReadOnly 191
Uso de la política 191
Información de la política 191
Versión de la política 191
Documento de política JSON 191
Más información 192

AmazonChimeSDK ... 192
Uso de la política ... 192
Información de la política ... 192
Versión de la política ... 192
Documento de política JSON ... 193
Más información ... 194
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy ... 194
Uso de la política ... 194
Información de la política ... 194
Versión de la política ... 194
Documento de política JSON ... 195
Más información ... 196
AmazonChimeSDKMessagingServiceRolePolicy ... 196
Uso de la política ... 196
Información de la política ... 196
Versión de la política ... 197
Documento de política JSON ... 197
Más información ... 198
AmazonChimeServiceRolePolicy ... 198
Uso de la política ... 198
Información de la política ... 198
Versión de la política ... 198
Documento de política JSON ... 198
Más información ... 199
AmazonChimeTranscriptionServiceLinkedRolePolicy ... 199
Uso de la política ... 199
Información de la política ... 199
Versión de la política ... 200
Documento de política JSON ... 200
Más información ... 200
AmazonChimeUserManagement ... 201
Uso de la política ... 201
Información de la política ... 201
Versión de la política ... 201
Documento de política JSON ... 201
Más información ... 202

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 203
Uso de la política 203
Información de la política 203
Versión de la política 203
Documento de política JSON 203
Más información 205
AmazonCloudDirectoryFullAccess 205
Uso de la política 206
Información de la política 206
Versión de la política 206
Documento de política JSON 206
Más información 207
AmazonCloudDirectoryReadOnlyAccess 207
Uso de la política 207
Información de la política 207
Versión de la política 207
Documento de política JSON 207
Más información 208
AmazonCloudWatchEvidentlyFullAccess 208
Uso de la política 208
Información de la política 209
Versión de la política 209
Documento de política JSON 209
Más información 211
AmazonCloudWatchEvidentlyReadOnlyAccess 212
Uso de la política 212
Información de la política 212
Versión de la política 212
Documento de política JSON 212
Más información 213
AmazonCloudWatchEvidentlyServiceRolePolicy 213
Uso de la política 213
Información de la política 213
Versión de la política 214
Documento de política JSON 214
Más información 215

AmazonCloudWatchRUMFullAccess 215
Uso de la política 216
Información de la política 216
Versión de la política 216
Documento de política JSON 216
Más información 219
AmazonCloudWatchRUMReadOnlyAccess 219
Uso de la política 219
Información de la política 219
Versión de la política 219
Documento de política JSON 219
Más información 221
AmazonCloudWatchRUMServiceRolePolicy 221
Uso de la política 221
Información de la política 221
Versión de la política 222
Documento de política JSON 222
Más información 222
AmazonCodeCatalystFullAccess 223
Uso de la política 223
Información de la política 223
Versión de la política 223
Documento de política JSON 223
Más información 224
AmazonCodeCatalystReadOnlyAccess 224
Uso de la política 224
Información de la política 225
Versión de la política 225
Documento de política JSON 225
Más información 225
AmazonCodeCatalystSupportAccess 226
Uso de la política 226
Información de la política 226
Versión de la política 226
Documento de política JSON 226
Más información 227

AmazonCodeGuruProfilerAgentAccess 227
Uso de la política 227
Información de la política 228
Versión de la política 228
Documento de política JSON 228
Más información 228
AmazonCodeGuruProfilerFullAccess 229
Uso de la política 229
Información de la política 229
Versión de la política 229
Documento de política JSON 229
Más información 230
AmazonCodeGuruProfilerReadOnlyAccess 230
Uso de la política 230
Información de la política 231
Versión de la política 231
Documento de política JSON 231
Más información 232
AmazonCodeGuruReviewerFullAccess 232
Uso de la política 232
Información de la política 232
Versión de la política 232
Documento de política JSON 233
Más información 235
AmazonCodeGuruReviewerReadOnlyAccess 235
Uso de la política 236
Información de la política 236
Versión de la política 236
Documento de política JSON 236
Más información 237
AmazonCodeGuruReviewerServiceRolePolicy 237
Uso de la política 237
Información de la política 237
Versión de la política 237
Documento de política JSON 238
Más información 240

AmazonCodeGuruSecurityFullAccess 240
Uso de la política 240
Información de la política 240
Versión de la política 240
Documento de política JSON 240
Más información 241
AmazonCodeGuruSecurityScanAccess 241
Uso de la política 241
Información de la política 241
Versión de la política 242
Documento de política JSON 242
Más información 242
AmazonCognitoDeveloperAuthenticatedIdentities 243
Uso de la política 243
Información de la política 243
Versión de la política 243
Documento de política JSON 243
Más información 244
AmazonCognitoIdpEmailServiceRolePolicy 244
Uso de la política 244
Información de la política 244
Versión de la política 245
Documento de política JSON 245
Más información 245
AmazonCognitoIdpServiceRolePolicy 246
Uso de la política 246
Información de la política 246
Versión de la política 246
Documento de política JSON 246
Más información 247
AmazonCognitoPowerUser 247
Uso de la política 247
Información de la política 247
Versión de la política 247
Documento de política JSON 248
Más información 249

AmazonCognitoReadOnly 249
Uso de la política 249
Información de la política 249
Versión de la política 250
Documento de política JSON 250
Más información 251
AmazonCognitoUnAuthedIdentitiesSessionPolicy 251
Uso de la política 251
Información de la política 251
Versión de la política 252
Documento de política JSON 252
Más información 253
AmazonCognitoUnauthenticatedIdentities 253
Uso de la política 253
Información de la política 253
Versión de la política 254
Documento de política JSON 254
Más información 254
AmazonConnect_FullAccess 254
Uso de la política 255
Información de la política 255
Versión de la política 255
Documento de política JSON 255
Más información 258
AmazonConnectCampaignsServiceLinkedRolePolicy 258
Uso de la política 258
Información de la política 258
Versión de la política 258
Documento de política JSON 259
Más información 261
AmazonConnectReadOnlyAccess 261
Uso de la política 261
Información de la política 261
Versión de la política 261
Documento de política JSON 261
Más información 262

AmazonConnectServiceLinkedRolePolicy 262
Uso de la política 262
Información de la política 263
Versión de la política 263
Documento de política JSON 263
Más información 273
AmazonConnectSynchronizationServiceRolePolicy 274
Uso de la política 274
Información de la política 274
Versión de la política 274
Documento de política JSON 274
Más información 276
AmazonConnectVoiceIDFullAccess 276
Uso de la política 276
Información de la política 276
Versión de la política 277
Documento de política JSON 277
Más información 277
AmazonDataZoneBedrockModelConsumptionPolicy 278
Uso de la política 278
Información de la política 278
Versión de la política 278
Documento de política JSON 278
Más información 281
AmazonDataZoneBedrockModelManagementPolicy 281
Uso de la política 281
Información de la política 281
Versión de la política 281
Documento de política JSON 282
Más información 283
AmazonDataZoneDomainExecutionRolePolicy 284
Uso de la política 284
Información de la política 284
Versión de la política 284
Documento de política JSON 284
Más información 288

AmazonDataZoneEnvironmentRolePermissionsBoundary 288
Uso de la política 288
Información de la política 289
Versión de la política 289
Documento de política JSON 289
Más información 302
AmazonDataZoneFullAccess 302
Uso de la política 302
Información de la política 302
Versión de la política 303
Documento de política JSON 303
Más información 312
AmazonDataZoneFullUserAccess 312
Uso de la política 312
Información de la política 312
Versión de la política 312
Documento de política JSON 313
Más información 316
AmazonDataZoneGlueManageAccessRolePolicy 316
Uso de la política 316
Información de la política 317
Versión de la política 317
Documento de política JSON 317
Más información 325
AmazonDataZonePortalFullAccessPolicy 325
Uso de la política 325
Información de la política 325
Versión de la política 325
Documento de política JSON 326
Más información 326
AmazonDataZonePreviewConsoleFullAccess 326
Uso de la política 326
Información de la política 327
Versión de la política 327
Documento de política JSON 327
Más información 329

AmazonDataZoneProjectDeploymentPermissionsBoundary 329
Uso de la política 329
Información de la política 329
Versión de la política 330
Documento de política JSON 330
Más información 338
AmazonDataZoneProjectRolePermissionsBoundary 338
Uso de la política 338
Información de la política 338
Versión de la política 339
Documento de política JSON 339
Más información 346
AmazonDataZoneRedshiftGlueProvisioningPolicy 346
Uso de la política 346
Información de la política 347
Versión de la política 347
Documento de política JSON 347
Más información 355
AmazonDataZoneRedshiftManageAccessRolePolicy 355
Uso de la política 355
Información de la política 355
Versión de la política 355
Documento de política JSON 356
Más información 359
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 359
Uso de la política 359
Información de la política 359
Versión de la política 360
Documento de política JSON 360
Más información 387
AmazonDataZoneSageMakerManageAccessRolePolicy 387
Uso de la política 388
Información de la política 388
Versión de la política 388
Documento de política JSON 388
Más información 393

AmazonDataZoneSageMakerProvisioningRolePolicy 393
Uso de la política 393
Información de la política 393
Versión de la política 393
Documento de política JSON 394
Más información 398
AmazonDetectiveFullAccess 399
Uso de la política 399
Información de la política 399
Versión de la política 399
Documento de política JSON 399
Más información 400
AmazonDetectiveInvestigatorAccess 400
Uso de la política 401
Información de la política 401
Versión de la política 401
Documento de política JSON 401
Más información 403
AmazonDetectiveMemberAccess 403
Uso de la política 403
Información de la política 403
Versión de la política 403
Documento de política JSON 404
Más información 404
AmazonDetectiveOrganizationsAccess 404
Uso de la política 405
Información de la política 405
Versión de la política 405
Documento de política JSON 405
Más información 407
AmazonDetectiveServiceLinkedRolePolicy 407
Uso de la política 407
Información de la política 407
Versión de la política 407
Documento de política JSON 408
Más información 408

AmazonDevOpsGuruConsoleFullAccess 408
Uso de la política 408
Información de la política 408
Versión de la política 409
Documento de política JSON 409
Más información 411
AmazonDevOpsGuruFullAccess 412
Uso de la política 412
Información de la política 412
Versión de la política 412
Documento de política JSON 412
Más información 414
AmazonDevOpsGuruOrganizationsAccess 415
Uso de la política 415
Información de la política 415
Versión de la política 415
Documento de política JSON 415
Más información 417
AmazonDevOpsGuruReadOnlyAccess 417
Uso de la política 417
Información de la política 417
Versión de la política 417
Documento de política JSON 417
Más información 419
AmazonDevOpsGuruServiceRolePolicy 420
Uso de la política 420
Información de la política 420
Versión de la política 420
Documento de política JSON 420
Más información 424
AmazonDMSCloudWatchLogsRole 424
Uso de la política 425
Información de la política 425
Versión de la política 425
Documento de política JSON 425
Más información 427

AmazonDMSRedshiftS3Role 427
Uso de la política 427
Información de la política 427
Versión de la política 427
Documento de política JSON 428
Más información 428
AmazonDMSVPCManagementRole 429
Uso de la política 429
Información de la política 429
Versión de la política 429
Documento de política JSON 429
Más información 430
AmazonDocDB-ElasticServiceRolePolicy 430
Uso de la política 430
Información de la política 430
Versión de la política 431
Documento de política JSON 431
Más información 431
AmazonDocDBConsoleFullAccess 431
Uso de la política 432
Información de la política 432
Versión de la política 432
Documento de política JSON 432
Más información 437
AmazonDocDBElasticFullAccess 437
Uso de la política 437
Información de la política 437
Versión de la política 437
Documento de política JSON 438
Más información 441
AmazonDocDBElasticReadOnlyAccess 441
Uso de la política 441
Información de la política 441
Versión de la política 442
Documento de política JSON 442
Más información 442

AmazonDocDBFullAccess 443
Uso de la política 443
Información de la política 443
Versión de la política 443
Documento de política JSON 443
Más información 446
AmazonDocDBReadOnlyAccess 446
Uso de la política 446
Información de la política 447
Versión de la política 447
Documento de política JSON 447
Más información 449
AmazonDRSVPCManagement 449
Uso de la política 449
Información de la política 449
Versión de la política 449
Documento de política JSON 450
Más información 450
AmazonDynamoDBFullAccess 451
Uso de la política 451
Información de la política 451
Versión de la política 451
Documento de política JSON 451
Más información 454
AmazonDynamoDBFullAccess_v2 454
Uso de la política 454
Información de la política 454
Versión de la política 454
Documento de política JSON 455
Más información 458
AmazonDynamoDBFullAccesswithDataPipeline 458
Uso de la política 458
Información de la política 459
Versión de la política 459
Documento de política JSON 459
Más información 461

AmazonDynamoDBReadOnlyAccess 461
Uso de la política 461
Información de la política 462
Versión de la política 462
Documento de política JSON 462
Más información 464
AmazonEBSCSIDriverPolicy 464
Uso de la política 464
Información de la política 464
Versión de la política 464
Documento de política JSON 465
Más información 469
AmazonEC2ContainerRegistryFullAccess 469
Uso de la política 469
Información de la política 469
Versión de la política 469
Documento de política JSON 470
Más información 470
AmazonEC2ContainerRegistryPowerUser 471
Uso de la política 471
Información de la política 471
Versión de la política 471
Documento de política JSON 471
Más información 472
AmazonEC2ContainerRegistryPullOnly 472
Uso de la política 472
Información de la política 473
Versión de la política 473
Documento de política JSON 473
Más información 473
AmazonEC2ContainerRegistryReadOnly 474
Uso de la política 474
Información de la política 474
Versión de la política 474
Documento de política JSON 474
Más información 475

AmazonEC2ContainerServiceAutoscaleRole 475
Uso de la política 475
Información de la política 476
Versión de la política 476
Documento de política JSON 476
Más información 477
AmazonEC2ContainerServiceEventsRole 477
Uso de la política 477
Información de la política 477
Versión de la política 477
Documento de política JSON 478
Más información 479
AmazonEC2ContainerServiceforEC2Role 479
Uso de la política 479
Información de la política 479
Versión de la política 479
Documento de política JSON 480
Más información 481
AmazonEC2ContainerServiceRole 481
Uso de la política 481
Información de la política 481
Versión de la política 481
Documento de política JSON 481
Más información 482
AmazonEC2FullAccess 482
Uso de la política 482
Información de la política 482
Versión de la política 483
Documento de política JSON 483
Más información 484
AmazonEC2ReadOnlyAccess 484
Uso de la política 484
Información de la política 484
Versión de la política 485
Documento de política JSON 485
Más información 486

AmazonEC2RoleforAWSCodeDeploy 486
Uso de la política 486
Información de la política 486
Versión de la política 486
Documento de política JSON 487
Más información 487
AmazonEC2RoleforAWSCodeDeployLimited 487
Uso de la política 488
Información de la política 488
Versión de la política 488
Documento de política JSON 488
Más información 489
AmazonEC2RoleforDataPipelineRole 489
Uso de la política 489
Información de la política 489
Versión de la política 490
Documento de política JSON 490
Más información 491
AmazonEC2RoleforSSM 491
Uso de la política 491
Información de la política 491
Versión de la política 491
Documento de política JSON 492
Más información 494
AmazonEC2RolePolicyForLaunchWizard 494
Uso de la política 494
Información de la política 494
Versión de la política 495
Documento de política JSON 495
Más información 499
AmazonEC2SpotFleetAutoscaleRole 499
Uso de la política 499
Información de la política 499
Versión de la política 499
Documento de política JSON 500
Más información 501

AmazonEC2SpotFleetTaggingRole 501
Uso de la política 501
Información de la política 501
Versión de la política 501
Documento de política JSON 502
Más información 503
AmazonECS_FullAccess 503
Uso de la política 503
Información de la política 503
Versión de la política 504
Documento de política JSON 504
Más información 510
AmazonECSComputeServiceRolePolicy 510
Uso de la política 510
Información de la política 510
Versión de la política 510
Documento de política JSON 511
Más información 512
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 512
Uso de la política 512
Información de la política 513
Versión de la política 513
Documento de política JSON 513
Más información 515
AmazonECSInfrastructureRolePolicyForVolumes 515
Uso de la política 516
Información de la política 516
Versión de la política 516
Documento de política JSON 516
Más información 518
AmazonECSInfrastructureRolePolicyForVpcLattice 519
Uso de la política 519
Información de la política 519
Versión de la política 519
Documento de política JSON 519
Más información 521

AmazonECSServiceRolePolicy 521
Uso de la política 521
Información de la política 521
Versión de la política 521
Documento de política JSON 522
Más información 527
AmazonECSTaskExecutionRolePolicy 527
Uso de la política 527
Información de la política 527
Versión de la política 527
Documento de política JSON 527
Más información 528
AmazonEFSCSIDriverPolicy 528
Uso de la política 528
Información de la política 528
Versión de la política 529
Documento de política JSON 529
Más información 530
AmazonEKS_CNI_Policy 531
Uso de la política 531
Información de la política 531
Versión de la política 531
Documento de política JSON 531
Más información 532
AmazonEKSBlockStoragePolicy 533
Uso de la política 533
Información de la política 533
Versión de la política 533
Documento de política JSON 533
Más información 535
AmazonEKSClusterPolicy 536
Uso de la política 536
Información de la política 536
Versión de la política 536
Documento de política JSON 536
Más información 539

AmazonEKSComputePolicy 539
Uso de la política 539
Información de la política 539
Versión de la política 539
Documento de política JSON 540
Más información 542
AmazonEKSConnectorServiceRolePolicy 542
Uso de la política 543
Información de la política 543
Versión de la política 543
Documento de política JSON 543
Más información 545
AmazonEKSDashboardConsoleReadOnly 545
Uso de la política 545
Información de la política 545
Versión de la política 546
Documento de política JSON 546
Más información 547
AmazonEKSDashboardServiceRolePolicy 547
Uso de la política 547
Información de la política 547
Versión de la política 548
Documento de política JSON 548
Más información 548
AmazonEKSFargatePodExecutionRolePolicy 549
Uso de la política 549
Información de la política 549
Versión de la política 549
Documento de política JSON 549
Más información 550
AmazonEKSForFargateServiceRolePolicy 550
Uso de la política 550
Información de la política 550
Versión de la política 550
Documento de política JSON 551
Más información 551

AmazonEKSLoadBalancingPolicy 551
Uso de la política 552
Información de la política 552
Versión de la política 552
Documento de política JSON 552
Más información 558
AmazonEKSLocalOutpostClusterPolicy 558
Uso de la política 559
Información de la política 559
Versión de la política 559
Documento de política JSON 559
Más información 561
AmazonEKSLocalOutpostServiceRolePolicy 561
Uso de la política 561
Información de la política 561
Versión de la política 562
Documento de política JSON 562
Más información 568
AmazonEKSNetworkingPolicy 568
Uso de la política 568
Información de la política 568
Versión de la política 568
Documento de política JSON 568
Más información 570
AmazonEKSServicePolicy 570
Uso de la política 570
Información de la política 570
Versión de la política 571
Documento de política JSON 571
Más información 573
AmazonEKSServiceRolePolicy 573
Uso de la política 573
Información de la política 573
Versión de la política 574
Documento de política JSON 574
Más información 581

AmazonEKSVPCResourceController 581
Uso de la política 582
Información de la política 582
Versión de la política 582
Documento de política JSON 582
Más información 583
AmazonEKSWorkerNodeMinimalPolicy 583
Uso de la política 583
Información de la política 583
Versión de la política 584
Documento de política JSON 584
Más información 584
AmazonEKSWorkerNodePolicy 584
Uso de la política 585
Información de la política 585
Versión de la política 585
Documento de política JSON 585
Más información 586
AmazonElastiCacheFullAccess 586
Uso de la política 586
Información de la política 586
Versión de la política 586
Documento de política JSON 587
Más información 590
AmazonElastiCacheReadOnlyAccess 590
Uso de la política 590
Información de la política 590
Versión de la política 591
Documento de política JSON 591
Más información 591
AmazonElasticContainerRegistryPublicFullAccess 591
Uso de la política 592
Información de la política 592
Versión de la política 592
Documento de política JSON 592
Más información 593

AmazonElasticContainerRegistryPublicPowerUser 593
Uso de la política 593
Información de la política 593
Versión de la política 593
Documento de política JSON 594
Más información 594
AmazonElasticContainerRegistryPublicReadOnly 595
Uso de la política 595
Información de la política 595
Versión de la política 595
Documento de política JSON 595
Más información 596
AmazonElasticFileSystemClientFullAccess 596
Uso de la política 596
Información de la política 596
Versión de la política 597
Documento de política JSON 597
Más información 597
AmazonElasticFileSystemClientReadOnlyAccess 597
Uso de la política 598
Información de la política 598
Versión de la política 598
Documento de política JSON 598
Más información 599
AmazonElasticFileSystemClientReadWriteAccess 599
Uso de la política 599
Información de la política 599
Versión de la política 599
Documento de política JSON 600
Más información 600
AmazonElasticFileSystemFullAccess 600
Uso de la política 600
Información de la política 600
Versión de la política 601
Documento de política JSON 601
Más información 603

AmazonElasticFileSystemReadOnlyAccess 603
Uso de la política 603
Información de la política 603
Versión de la política 604
Documento de política JSON 604
Más información 605
AmazonElasticFileSystemServiceRolePolicy 605
Uso de la política 605
Información de la política 605
Versión de la política 605
Documento de política JSON 606
Más información 608
AmazonElasticFileSystemsUtils 608
Uso de la política 608
Información de la política 608
Versión de la política 608
Documento de política JSON 609
Más información 610
AmazonElasticMapReduceEditorsRole 611
Uso de la política 611
Información de la política 611
Versión de la política 611
Documento de política JSON 611
Más información 612
AmazonElasticMapReduceforAutoScalingRole 613
Uso de la política 613
Información de la política 613
Versión de la política 613
Documento de política JSON 613
Más información 614
AmazonElasticMapReduceforEC2Role 614
Uso de la política 614
Información de la política 614
Versión de la política 615
Documento de política JSON 615
Más información 616

AmazonElasticMapReduceFullAccess 616
Uso de la política 617
Información de la política 617
Versión de la política 617
Documento de política JSON 617
Más información 619
AmazonElasticMapReducePlacementGroupPolicy 619
Uso de la política 619
Información de la política 619
Versión de la política 619
Documento de política JSON 620
Más información 620
AmazonElasticMapReduceReadOnlyAccess 621
Uso de la política 621
Información de la política 621
Versión de la política 621
Documento de política JSON 621
Más información 622
AmazonElasticMapReduceRole 622
Uso de la política 622
Información de la política 622
Versión de la política 623
Documento de política JSON 623
Más información 625
AmazonElasticsearchServiceRolePolicy 625
Uso de la política 625
Información de la política 625
Versión de la política 626
Documento de política JSON 626
Más información 629
AmazonElasticTranscoder_FullAccess 629
Uso de la política 629
Información de la política 629
Versión de la política 629
Documento de política JSON 629
Más información 630

AmazonElasticTranscoder_JobsSubmitter 631
Uso de la política 631
Información de la política 631
Versión de la política 631
Documento de política JSON 631
Más información 632
AmazonElasticTranscoder_ReadOnlyAccess 632
Uso de la política 632
Información de la política 632
Versión de la política 633
Documento de política JSON 633
Más información 633
AmazonElasticTranscoderRole 634
Uso de la política 634
Información de la política 634
Versión de la política 634
Documento de política JSON 634
Más información 635
AmazonEMRCleanupPolicy 635
Uso de la política 635
Información de la política 636
Versión de la política 636
Documento de política JSON 636
Más información 637
AmazonEMRContainersServiceRolePolicy 637
Uso de la política 637
Información de la política 637
Versión de la política 637
Documento de política JSON 638
Más información 639
AmazonEMRFullAccessPolicy_v2 639
Uso de la política 639
Información de la política 639
Versión de la política 639
Documento de política JSON 640
Más información 643

AmazonEMRReadOnlyAccessPolicy_v2 643
Uso de la política 643
Información de la política 643
Versión de la política 644
Documento de política JSON 644
Más información 645
AmazonEMRServerlessServiceRolePolicy 645
Uso de la política 645
Información de la política 645
Versión de la política 646
Documento de política JSON 646
Más información 647
AmazonEMRServicePolicy_v2 647
Uso de la política 647
Información de la política 647
Versión de la política 648
Documento de política JSON 648
Más información 656
AmazonESCognitoAccess 657
Uso de la política 657
Información de la política 657
Versión de la política 657
Documento de política JSON 657
Más información 658
AmazonESFullAccess 659
Uso de la política 659
Información de la política 659
Versión de la política 659
Documento de política JSON 659
Más información 660
AmazonESReadOnlyAccess 660
Uso de la política 660
Información de la política 660
Versión de la política 660
Documento de política JSON 660
Más información 661

AmazonEventBridgeApiDestinationsServiceRolePolicy 661
Uso de la política 661
Información de la política 661
Versión de la política 662
Documento de política JSON 662
Más información 663
AmazonEventBridgeFullAccess 663
Uso de la política 663
Información de la política 663
Versión de la política 664
Documento de política JSON 664
Más información 666
AmazonEventBridgePipesFullAccess 666
Uso de la política 666
Información de la política 666
Versión de la política 667
Documento de política JSON 667
Más información 667
AmazonEventBridgePipesOperatorAccess 668
Uso de la política 668
Información de la política 668
Versión de la política 668
Documento de política JSON 668
Más información 669
AmazonEventBridgePipesReadOnlyAccess 669
Uso de la política 669
Información de la política 669
Versión de la política 669
Documento de política JSON 670
Más información 670
AmazonEventBridgeReadOnlyAccess 670
Uso de la política 670
Información de la política 671
Versión de la política 671
Documento de política JSON 671
Más información 672

AmazonEventBridgeSchedulerFullAccess 673
Uso de la política 673
Información de la política 673
Versión de la política 673
Documento de política JSON 673
Más información 674
AmazonEventBridgeSchedulerReadOnlyAccess 674
Uso de la política 674
Información de la política 674
Versión de la política 675
Documento de política JSON 675
Más información 675
AmazonEventBridgeSchemasFullAccess 675
Uso de la política 676
Información de la política 676
Versión de la política 676
Documento de política JSON 676
Más información 677
AmazonEventBridgeSchemasReadOnlyAccess 677
Uso de la política 677
Información de la política 677
Versión de la política 678
Documento de política JSON 678
Más información 679
AmazonEventBridgeSchemasServiceRolePolicy 679
Uso de la política 679
Información de la política 679
Versión de la política 679
Documento de política JSON 680
Más información 680
AmazonEVSServiceRolePolicy 680
Uso de la política 680
Información de la política 681
Versión de la política 681
Documento de política JSON 681
Más información 683

AmazonFISServiceRolePolicy 683
Uso de la política 683
Información de la política 683
Versión de la política 684
Documento de política JSON 684
Más información 685
AmazonForecastFullAccess 686
Uso de la política 686
Información de la política 686
Versión de la política 686
Documento de política JSON 686
Más información 687
AmazonFraudDetectorFullAccessPolicy 687
Uso de la política 687
Información de la política 687
Versión de la política 688
Documento de política JSON 688
Más información 689
AmazonFreeRTOSFullAccess 689
Uso de la política 689
Información de la política 689
Versión de la política 690
Documento de política JSON 690
Más información 690
AmazonFreeRTOSOTAUpdate 690
Uso de la política 691
Información de la política 691
Versión de la política 691
Documento de política JSON 691
Más información 693
AmazonFSxConsoleFullAccess 693
Uso de la política 693
Información de la política 693
Versión de la política 693
Documento de política JSON 694
Más información 697

AmazonFSxConsoleReadOnlyAccess 697
Uso de la política 697
Información de la política 698
Versión de la política 698
Documento de política JSON 698
Más información 699
AmazonFSxFullAccess 699
Uso de la política 699
Información de la política 699
Versión de la política 699
Documento de política JSON 700
Más información 704
AmazonFSxReadOnlyAccess 704
Uso de la política 704
Información de la política 704
Versión de la política 704
Documento de política JSON 705
Más información 705
AmazonFSxServiceRolePolicy 705
Uso de la política 705
Información de la política 705
Versión de la política 706
Documento de política JSON 706
Más información 709
AmazonGlacierFullAccess 709
Uso de la política 709
Información de la política 709
Versión de la política 709
Documento de política JSON 709
Más información 710
AmazonGlacierReadOnlyAccess 710
Uso de la política 710
Información de la política 710
Versión de la política 711
Documento de política JSON 711
Más información 711

AmazonGrafanaAthenaAccess 712
Uso de la política 712
Información de la política 712
Versión de la política 712
Documento de política JSON 712
Más información 714
AmazonGrafanaCloudWatchAccess 714
Uso de la política 714
Información de la política 715
Versión de la política 715
Documento de política JSON 715
Más información 716
AmazonGrafanaRedshiftAccess 717
Uso de la política 717
Información de la política 717
Versión de la política 717
Documento de política JSON 717
Más información 718
AmazonGrafanaServiceLinkedRolePolicy 719
Uso de la política 719
Información de la política 719
Versión de la política 719
Documento de política JSON 719
Más información 721
AmazonGuardDutyFullAccess 721
Uso de la política 721
Información de la política 721
Versión de la política 721
Documento de política JSON 721
Más información 723
AmazonGuardDutyFullAccess_v2 723
Uso de la política 723
Información de la política 723
Versión de la política 724
Documento de política JSON 724
Más información 726

AmazonGuardDutyMalwareProtectionServiceRolePolicy 726
Uso de la política 726
Información de la política 726
Versión de la política 727
Documento de política JSON 727
Más información 731
AmazonGuardDutyReadOnlyAccess 731
Uso de la política 732
Información de la política 732
Versión de la política 732
Documento de política JSON 732
Más información 733
AmazonGuardDutyServiceRolePolicy 733
Uso de la política 733
Información de la política 733
Versión de la política 734
Documento de política JSON 734
Más información 740
AmazonHealthLakeFullAccess 740
Uso de la política 740
Información de la política 740
Versión de la política 740
Documento de política JSON 741
Más información 741
AmazonHealthLakeReadOnlyAccess 742
Uso de la política 742
Información de la política 742
Versión de la política 742
Documento de política JSON 742
Más información 743
AmazonHoneycodeFullAccess 743
Uso de la política 743
Información de la política 743
Versión de la política 743
Documento de política JSON 744
Más información 744

AmazonHoneycodeReadOnlyAccess 744
Uso de la política 744
Información de la política 745
Versión de la política 745
Documento de política JSON 745
Más información 745
AmazonHoneycodeServiceRolePolicy 746
Uso de la política 746
Información de la política 746
Versión de la política 746
Documento de política JSON 746
Más información 747
AmazonHoneycodeTeamAssociationFullAccess 747
Uso de la política 747
Información de la política 747
Versión de la política 747
Documento de política JSON 748
Más información 748
AmazonHoneycodeTeamAssociationReadOnlyAccess 748
Uso de la política 749
Información de la política 749
Versión de la política 749
Documento de política JSON 749
Más información 749
AmazonHoneycodeWorkbookFullAccess 750
Uso de la política 750
Información de la política 750
Versión de la política 750
Documento de política JSON 750
Más información 751
AmazonHoneycodeWorkbookReadOnlyAccess 751
Uso de la política 751
Información de la política 752
Versión de la política 752
Documento de política JSON 752
Más información 752

AmazonInspector2AgentlessServiceRolePolicy 753
Uso de la política 753
Información de la política 753
Versión de la política 753
Documento de política JSON 753
Más información 757
AmazonInspector2FullAccess 757
Uso de la política 757
Información de la política 757
Versión de la política 758
Documento de política JSON 758
Más información 759
AmazonInspector2FullAccess_v2 759
Uso de la política 759
Información de la política 760
Versión de la política 760
Documento de política JSON 760
Más información 762
AmazonInspector2ManagedCisPolicy 762
Uso de la política 762
Información de la política 762
Versión de la política 763
Documento de política JSON 763
Más información 763
AmazonInspector2ReadOnlyAccess 764
Uso de la política 764
Información de la política 764
Versión de la política 764
Documento de política JSON 764
Más información 765
AmazonInspector2ServiceRolePolicy 765
Uso de la política 765
Información de la política 765
Versión de la política 766
Documento de política JSON 766
Más información 773

AmazonInspectorFullAccess 773
Uso de la política 773
Información de la política 774
Versión de la política 774
Documento de política JSON 774
Más información 775
AmazonInspectorReadOnlyAccess 775
Uso de la política 775
Información de la política 776
Versión de la política 776
Documento de política JSON 776
Más información 777
AmazonInspectorServiceRolePolicy 777
Uso de la política 777
Información de la política 777
Versión de la política 777
Documento de política JSON 778
Más información 779
AmazonKendraFullAccess 779
Uso de la política 779
Información de la política 779
Versión de la política 780
Documento de política JSON 780
Más información 782
AmazonKendraReadOnlyAccess 782
Uso de la política 782
Información de la política 782
Versión de la política 782
Documento de política JSON 783
Más información 783
AmazonKeyspacesFullAccess 783
Uso de la política 783
Información de la política 784
Versión de la política 784
Documento de política JSON 784
Más información 786

AmazonKeyspacesReadOnlyAccess 786
Uso de la política 786
Información de la política 787
Versión de la política 787
Documento de política JSON 787
Más información 788
AmazonKeyspacesReadOnlyAccess_v2 788
Uso de la política 788
Información de la política 788
Versión de la política 789
Documento de política JSON 789
Más información 790
AmazonKinesisAnalyticsFullAccess 790
Uso de la política 790
Información de la política 790
Versión de la política 790
Documento de política JSON 791
Más información 792
AmazonKinesisAnalyticsReadOnly 792
Uso de la política 792
Información de la política 793
Versión de la política 793
Documento de política JSON 793
Más información 794
AmazonKinesisFirehoseFullAccess 795
Uso de la política 795
Información de la política 795
Versión de la política 795
Documento de política JSON 795
Más información 796
AmazonKinesisFirehoseReadOnlyAccess 796
Uso de la política 796
Información de la política 796
Versión de la política 796
Documento de política JSON 797
Más información 797

AmazonKinesisFullAccess 797
Uso de la política 797
Información de la política 797
Versión de la política 798
Documento de política JSON 798
Más información 798
AmazonKinesisReadOnlyAccess 799
Uso de la política 799
Información de la política 799
Versión de la política 799
Documento de política JSON 799
Más información 800
AmazonKinesisVideoStreamsFullAccess 800
Uso de la política 800
Información de la política 800
Versión de la política 800
Documento de política JSON 801
Más información 801
AmazonKinesisVideoStreamsReadOnlyAccess 801
Uso de la política 801
Información de la política 801
Versión de la política 802
Documento de política JSON 802
Más información 802
AmazonLaunchWizard_Fullaccess 803
Uso de la política 803
Información de la política 803
Versión de la política 803
Documento de política JSON 803
Más información 817
AmazonLaunchWizardFullAccessV2 818
Uso de la política 818
Información de la política 818
Versión de la política 818
Documento de política JSON 818
Más información 835

AmazonLexChannelsAccess 835
Uso de la política 835
Información de la política 835
Versión de la política 836
Documento de política JSON 836
Más información 836
AmazonLexFullAccess 836
Uso de la política 836
Información de la política 837
Versión de la política 837
Documento de política JSON 837
Más información 842
AmazonLexReadOnly 843
Uso de la política 843
Información de la política 843
Versión de la política 843
Documento de política JSON 843
Más información 845
AmazonLexReplicationPolicy 845
Uso de la política 845
Información de la política 845
Versión de la política 846
Documento de política JSON 846
Más información 848
AmazonLexRunBotsOnly 848
Uso de la política 848
Información de la política 848
Versión de la política 849
Documento de política JSON 849
Más información 849
AmazonLexV2BotPolicy 850
Uso de la política 850
Información de la política 850
Versión de la política 850
Documento de política JSON 850
Más información 851

AmazonLookoutEquipmentFullAccess 851
Uso de la política 851
Información de la política 851
Versión de la política 851
Documento de política JSON 852
Más información 853
AmazonLookoutEquipmentReadOnlyAccess 853
Uso de la política 853
Información de la política 853
Versión de la política 854
Documento de política JSON 854
Más información 854
AmazonLookoutMetricsFullAccess 854
Uso de la política 855
Información de la política 855
Versión de la política 855
Documento de política JSON 855
Más información 856
AmazonLookoutMetricsReadOnlyAccess 856
Uso de la política 856
Información de la política 856
Versión de la política 856
Documento de política JSON 857
Más información 857
AmazonLookoutVisionConsoleFullAccess 858
Uso de la política 858
Información de la política 858
Versión de la política 858
Documento de política JSON 858
Más información 861
AmazonLookoutVisionConsoleReadOnlyAccess 861
Uso de la política 861
Información de la política 861
Versión de la política 861
Documento de política JSON 862
Más información 863

AmazonLookoutVisionFullAccess 863
Uso de la política 863
Información de la política 863
Versión de la política 864
Documento de política JSON 864
Más información 864
AmazonLookoutVisionReadOnlyAccess 864
Uso de la política 865
Información de la política 865
Versión de la política 865
Documento de política JSON 865
Más información 866
AmazonMachineLearningBatchPredictionsAccess 866
Uso de la política 866
Información de la política 866
Versión de la política 866
Documento de política JSON 867
Más información 867
AmazonMachineLearningCreateOnlyAccess 867
Uso de la política 868
Información de la política 868
Versión de la política 868
Documento de política JSON 868
Más información 869
AmazonMachineLearningFullAccess 869
Uso de la política 869
Información de la política 869
Versión de la política 869
Documento de política JSON 869
Más información 870
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 870
Uso de la política 870
Información de la política 870
Versión de la política 871
Documento de política JSON 871
Más información 871

AmazonMachineLearningReadOnlyAccess 872
Uso de la política 872
Información de la política 872
Versión de la política 872
Documento de política JSON 872
Más información 873
AmazonMachineLearningRealTimePredictionOnlyAccess 873
Uso de la política 873
Información de la política 873
Versión de la política 873
Documento de política JSON 874
Más información 874
AmazonMachineLearningRoleforRedshiftDataSourceV3 874
Uso de la política 874
Información de la política 875
Versión de la política 875
Documento de política JSON 875
Más información 876
AmazonMacieFullAccess 876
Uso de la política 876
Información de la política 876
Versión de la política 877
Documento de política JSON 877
Más información 878
AmazonMacieHandshakeRole 878
Uso de la política 878
Información de la política 878
Versión de la política 878
Documento de política JSON 878
Más información 879
AmazonMacieReadOnlyAccess 879
Uso de la política 879
Información de la política 879
Versión de la política 880
Documento de política JSON 880
Más información 880

AmazonMacieServiceRole 881
Uso de la política 881
Información de la política 881
Versión de la política 881
Documento de política JSON 881
Más información 882
AmazonMacieServiceRolePolicy 882
Uso de la política 882
Información de la política 882
Versión de la política 882
Documento de política JSON 883
Más información 884
AmazonManagedBlockchainConsoleFullAccess 884
Uso de la política 884
Información de la política 884
Versión de la política 885
Documento de política JSON 885
Más información 885
AmazonManagedBlockchainFullAccess 886
Uso de la política 886
Información de la política 886
Versión de la política 886
Documento de política JSON 886
Más información 887
AmazonManagedBlockchainReadOnlyAccess 887
Uso de la política 887
Información de la política 887
Versión de la política 887
Documento de política JSON 888
Más información 888
AmazonManagedBlockchainServiceRolePolicy 888
Uso de la política 888
Información de la política 889
Versión de la política 889
Documento de política JSON 889
Más información 890

AmazonMCSFullAccess 890
Uso de la política 890
Información de la política 890
Versión de la política 890
Documento de política JSON 890
Más información 892
AmazonMCSReadOnlyAccess 892
Uso de la política 892
Información de la política 892
Versión de la política 892
Documento de política JSON 893
Más información 893
AmazonMechanicalTurkFullAccess 893
Uso de la política 894
Información de la política 894
Versión de la política 894
Documento de política JSON 894
Más información 895
AmazonMechanicalTurkReadOnly 895
Uso de la política 895
Información de la política 895
Versión de la política 895
Documento de política JSON 895
Más información 896
AmazonMemoryDBFullAccess 896
Uso de la política 896
Información de la política 896
Versión de la política 897
Documento de política JSON 897
Más información 897
AmazonMemoryDBReadOnlyAccess 898
Uso de la política 898
Información de la política 898
Versión de la política 898
Documento de política JSON 898
Más información 899

AmazonMobileAnalyticsFinancialReportAccess 899
Uso de la política 899
Información de la política 899
Versión de la política 900
Documento de política JSON 900
Más información 900
AmazonMobileAnalyticsFullAccess 900
Uso de la política 901
Información de la política 901
Versión de la política 901
Documento de política JSON 901
Más información 901
AmazonMobileAnalyticsNon-financialReportAccess 902
Uso de la política 902
Información de la política 902
Versión de la política 902
Documento de política JSON 902
Más información 903
AmazonMobileAnalyticsWriteOnlyAccess 903
Uso de la política 903
Información de la política 903
Versión de la política 903
Documento de política JSON 904
Más información 904
AmazonMonitronFullAccess 904
Uso de la política 904
Información de la política 904
Versión de la política 905
Documento de política JSON 905
Más información 907
AmazonMQApiFullAccess 907
Uso de la política 907
Información de la política 907
Versión de la política 907
Documento de política JSON 908
Más información 909

AmazonMQApiReadOnlyAccess 909
Uso de la política 909
Información de la política 909
Versión de la política 909
Documento de política JSON 910
Más información 910
AmazonMQFullAccess 910
Uso de la política 911
Información de la política 911
Versión de la política 911
Documento de política JSON 911
Más información 912
AmazonMQReadOnlyAccess 913
Uso de la política 913
Información de la política 913
Versión de la política 913
Documento de política JSON 913
Más información 914
AmazonMQServiceRolePolicy 914
Uso de la política 914
Información de la política 914
Versión de la política 914
Documento de política JSON 915
Más información 916
AmazonMSKConnectReadOnlyAccess 917
Uso de la política 917
Información de la política 917
Versión de la política 917
Documento de política JSON 917
Más información 918
AmazonMSKFullAccess 919
Uso de la política 919
Información de la política 919
Versión de la política 919
Documento de política JSON 919
Más información 922

AmazonMSKReadOnlyAccess 922
Uso de la política 922
Información de la política 922
Versión de la política 923
Documento de política JSON 923
Más información 923
AmazonMWAAServiceRolePolicy 924
Uso de la política 924
Información de la política 924
Versión de la política 924
Documento de política JSON 924
Más información 927
AmazonNimbleStudio-LaunchProfileWorker 927
Uso de la política 927
Información de la política 927
Versión de la política 927
Documento de política JSON 927
Más información 928
AmazonNimbleStudio-StudioAdmin 928
Uso de la política 928
Información de la política 929
Versión de la política 929
Documento de política JSON 929
Más información 931
AmazonNimbleStudio-StudioUser 931
Uso de la política 931
Información de la política 931
Versión de la política 932
Documento de política JSON 932
Más información 934
AmazonODBServiceRolePolicy 934
Uso de la política 934
Información de la política 934
Versión de la política 935
Documento de política JSON 935
Más información 936

AmazonOmicsFullAccess 936
Uso de la política 936
Información de la política 936
Versión de la política 937
Documento de política JSON 937
Más información 938
AmazonOmicsReadOnlyAccess 938
Uso de la política 938
Información de la política 938
Versión de la política 938
Documento de política JSON 939
Más información 939
AmazonOneEnterpriseFullAccess 939
Uso de la política 939
Información de la política 940
Versión de la política 940
Documento de política JSON 940
Más información 940
AmazonOneEnterpriseInstallerAccess 941
Uso de la política 941
Información de la política 941
Versión de la política 941
Documento de política JSON 941
Más información 942
AmazonOneEnterpriseReadOnlyAccess 942
Uso de la política 942
Información de la política 942
Versión de la política 943
Documento de política JSON 943
Más información 943
AmazonOpenSearchDashboardsServiceRolePolicy 943
Uso de la política 944
Información de la política 944
Versión de la política 944
Documento de política JSON 944
Más información 945

AmazonOpenSearchDirectQueryGlueCreateAccess 945
Uso de la política 945
Información de la política 945
Versión de la política 945
Documento de política JSON 946
Más información 946
AmazonOpenSearchIngestionFullAccess 946
Uso de la política 946
Información de la política 947
Versión de la política 947
Documento de política JSON 947
Más información 948
AmazonOpenSearchIngestionReadOnlyAccess 948
Uso de la política 948
Información de la política 948
Versión de la política 949
Documento de política JSON 949
Más información 949
AmazonOpenSearchIngestionServiceRolePolicy 950
Uso de la política 950
Información de la política 950
Versión de la política 950
Documento de política JSON 950
Más información 952
AmazonOpenSearchServerlessServiceRolePolicy 952
Uso de la política 952
Información de la política 953
Versión de la política 953
Documento de política JSON 953
Más información 953
AmazonOpenSearchServiceCognitoAccess 954
Uso de la política 954
Información de la política 954
Versión de la política 954
Documento de política JSON 954
Más información 955

AmazonOpenSearchServiceFullAccess 956
Uso de la política 956
Información de la política 956
Versión de la política 956
Documento de política JSON 956
Más información 957
AmazonOpenSearchServiceReadOnlyAccess 957
Uso de la política 957
Información de la política 957
Versión de la política 957
Documento de política JSON 958
Más información 958
AmazonOpenSearchServiceRolePolicy 958
Uso de la política 959
Información de la política 959
Versión de la política 959
Documento de política JSON 959
Más información 964
AmazonPersonalizeFullAccess 964
Uso de la política 964
Información de la política 964
Versión de la política 965
Documento de política JSON 965
Más información 966
AmazonPollyFullAccess 966
Uso de la política 966
Información de la política 966
Versión de la política 967
Documento de política JSON 967
Más información 967
AmazonPollyReadOnlyAccess 967
Uso de la política 968
Información de la política 968
Versión de la política 968
Documento de política JSON 968
Más información 969

AmazonPrometheusConsoleFullAccess 969
Uso de la política 969
Información de la política 969
Versión de la política 969
Documento de política JSON 970
Más información 971
AmazonPrometheusFullAccess 971
Uso de la política 971
Información de la política 971
Versión de la política 971
Documento de política JSON 972
Más información 973
AmazonPrometheusQueryAccess 973
Uso de la política 973
Información de la política 973
Versión de la política 973
Documento de política JSON 974
Más información 974
AmazonPrometheusRemoteWriteAccess 974
Uso de la política 975
Información de la política 975
Versión de la política 975
Documento de política JSON 975
Más información 975
AmazonPrometheusScraperServiceRolePolicy 976
Uso de la política 976
Información de la política 976
Versión de la política 976
Documento de política JSON 976
Más información 979
AmazonQDeveloperAccess 979
Uso de la política 979
Información de la política 979
Versión de la política 979
Documento de política JSON 980
Más información 981

AmazonQFullAccess 981
Uso de la política 981
Información de la política 981
Versión de la política 981
Documento de política JSON 982
Más información 983
AmazonQLDBConsoleFullAccess 984
Uso de la política 984
Información de la política 984
Versión de la política 984
Documento de política JSON 984
Más información 986
AmazonQLDBFullAccess 986
Uso de la política 986
Información de la política 986
Versión de la política 987
Documento de política JSON 987
Más información 988
AmazonQLDBReadOnly 988
Uso de la política 989
Información de la política 989
Versión de la política 989
Documento de política JSON 989
Más información 990
AmazonRDSBetaServiceRolePolicy 990
Uso de la política 990
Información de la política 990
Versión de la política 990
Documento de política JSON 991
Más información 994
AmazonRDSCustomInstanceProfileRolePolicy 994
Uso de la política 994
Información de la política 994
Versión de la política 994
Documento de política JSON 994
Más información 1002

AmazonRDSCustomPreviewServiceRolePolicy 1002
Uso de la política 1002
Información de la política 1002
Versión de la política 1002
Documento de política JSON 1003
Más información 1019
AmazonRDSCustomServiceRolePolicy 1020
Uso de la política 1020
Información de la política 1020
Versión de la política 1020
Documento de política JSON 1020
Más información 1039
AmazonRDSDataFullAccess 1039
Uso de la política 1039
Información de la política 1039
Versión de la política 1039
Documento de política JSON 1040
Más información 1041
AmazonRDSDirectoryServiceAccess 1041
Uso de la política 1041
Información de la política 1041
Versión de la política 1041
Documento de política JSON 1042
Más información 1042
AmazonRDSEnhancedMonitoringRole 1042
Uso de la política 1043
Información de la política 1043
Versión de la política 1043
Documento de política JSON 1043
Más información 1044
AmazonRDSFullAccess 1044
Uso de la política 1044
Información de la política 1044
Versión de la política 1045
Documento de política JSON 1045
Más información 1047

AmazonRDSPerformanceInsightsFullAccess 1047
Uso de la política 1047
Información de la política 1047
Versión de la política 1048
Documento de política JSON 1048
Más información 1049
AmazonRDSPerformanceInsightsReadOnly 1049
Uso de la política 1050
Información de la política 1050
Versión de la política 1050
Documento de política JSON 1050
Más información 1052
AmazonRDSPreviewServiceRolePolicy 1052
Uso de la política 1052
Información de la política 1052
Versión de la política 1053
Documento de política JSON 1053
Más información 1056
AmazonRDSReadOnlyAccess 1056
Uso de la política 1056
Información de la política 1056
Versión de la política 1056
Documento de política JSON 1057
Más información 1058
AmazonRDSServiceRolePolicy 1058
Uso de la política 1058
Información de la política 1058
Versión de la política 1059
Documento de política JSON 1059
Más información 1063
AmazonRedshiftAllCommandsFullAccess 1063
Uso de la política 1063
Información de la política 1063
Versión de la política 1063
Documento de política JSON 1063
Más información 1069

AmazonRedshiftDataFullAccess 1069
Uso de la política 1069
Información de la política 1069
Versión de la política 1069
Documento de política JSON 1070
Más información 1072
AmazonRedshiftFullAccess 1072
Uso de la política 1072
Información de la política 1072
Versión de la política 1072
Documento de política JSON 1073
Más información 1075
AmazonRedshiftQueryEditor 1075
Uso de la política 1075
Información de la política 1075
Versión de la política 1075
Documento de política JSON 1076
Más información 1077
AmazonRedshiftQueryEditorV2FullAccess 1078
Uso de la política 1078
Información de la política 1078
Versión de la política 1078
Documento de política JSON 1078
Más información 1080
AmazonRedshiftQueryEditorV2NoSharing 1080
Uso de la política 1080
Información de la política 1080
Versión de la política 1081
Documento de política JSON 1081
Más información 1084
AmazonRedshiftQueryEditorV2ReadSharing 1085
Uso de la política 1085
Información de la política 1085
Versión de la política 1085
Documento de política JSON 1085
Más información 1090

AmazonRedshiftQueryEditorV2ReadWriteSharing 1090
Uso de la política 1091
Información de la política 1091
Versión de la política 1091
Documento de política JSON 1091
Más información 1096
AmazonRedshiftReadOnlyAccess 1096
Uso de la política 1097
Información de la política 1097
Versión de la política 1097
Documento de política JSON 1097
Más información 1098
AmazonRedshiftServiceLinkedRolePolicy 1098
Uso de la política 1098
Información de la política 1098
Versión de la política 1099
Documento de política JSON 1099
Más información 1105
AmazonRekognitionCustomLabelsFullAccess 1105
Uso de la política 1105
Información de la política 1105
Versión de la política 1106
Documento de política JSON 1106
Más información 1107
AmazonRekognitionFullAccess 1107
Uso de la política 1107
Información de la política 1108
Versión de la política 1108
Documento de política JSON 1108
Más información 1108
AmazonRekognitionReadOnlyAccess 1109
Uso de la política 1109
Información de la política 1109
Versión de la política 1109
Documento de política JSON 1109
Más información 1110

AmazonRekognitionServiceRole 1111
Uso de la política 1111
Información de la política 1111
Versión de la política 1111
Documento de política JSON 1111
Más información 1112
AmazonRoute53AutoNamingFullAccess 1112
Uso de la política 1112
Información de la política 1113
Versión de la política 1113
Documento de política JSON 1113
Más información 1114
AmazonRoute53AutoNamingReadOnlyAccess 1114
Uso de la política 1114
Información de la política 1114
Versión de la política 1114
Documento de política JSON 1115
Más información 1115
AmazonRoute53AutoNamingRegistrantAccess 1115
Uso de la política 1115
Información de la política 1116
Versión de la política 1116
Documento de política JSON 1116
Más información 1117
AmazonRoute53DomainsFullAccess 1117
Uso de la política 1117
Información de la política 1117
Versión de la política 1117
Documento de política JSON 1118
Más información 1118
AmazonRoute53DomainsReadOnlyAccess 1118
Uso de la política 1118
Información de la política 1119
Versión de la política 1119
Documento de política JSON 1119
Más información 1119

AmazonRoute53FullAccess 1120
Uso de la política 1120
Información de la política 1120
Versión de la política 1120
Documento de política JSON 1120
Más información 1121
AmazonRoute53ProfilesFullAccess 1122
Uso de la política 1122
Información de la política 1122
Versión de la política 1122
Documento de política JSON 1122
Más información 1123
AmazonRoute53ProfilesReadOnlyAccess 1123
Uso de la política 1124
Información de la política 1124
Versión de la política 1124
Documento de política JSON 1124
Más información 1125
AmazonRoute53ReadOnlyAccess 1125
Uso de la política 1125
Información de la política 1125
Versión de la política 1126
Documento de política JSON 1126
Más información 1126
AmazonRoute53RecoveryClusterFullAccess 1126
Uso de la política 1127
Información de la política 1127
Versión de la política 1127
Documento de política JSON 1127
Más información 1128
AmazonRoute53RecoveryClusterReadOnlyAccess 1128
Uso de la política 1128
Información de la política 1128
Versión de la política 1128
Documento de política JSON 1129
Más información 1129

AmazonRoute53RecoveryControlConfigFullAccess 1129
Uso de la política 1129
Información de la política 1129
Versión de la política 1130
Documento de política JSON 1130
Más información 1130
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1131
Uso de la política 1131
Información de la política 1131
Versión de la política 1131
Documento de política JSON 1131
Más información 1132
AmazonRoute53RecoveryReadinessFullAccess 1132
Uso de la política 1132
Información de la política 1132
Versión de la política 1133
Documento de política JSON 1133
Más información 1133
AmazonRoute53RecoveryReadinessReadOnlyAccess 1133
Uso de la política 1134
Información de la política 1134
Versión de la política 1134
Documento de política JSON 1134
Más información 1135
AmazonRoute53ResolverFullAccess 1135
Uso de la política 1135
Información de la política 1135
Versión de la política 1136
Documento de política JSON 1136
Más información 1137
AmazonRoute53ResolverReadOnlyAccess 1137
Uso de la política 1137
Información de la política 1137
Versión de la política 1137
Documento de política JSON 1137
Más información 1138

AmazonS3FullAccess 1138
Uso de la política 1138
Información de la política 1139
Versión de la política 1139
Documento de política JSON 1139
Más información 1139
AmazonS3ObjectLambdaExecutionRolePolicy 1140
Uso de la política 1140
Información de la política 1140
Versión de la política 1140
Documento de política JSON 1140
Más información 1141
AmazonS3OutpostsFullAccess 1141
Uso de la política 1141
Información de la política 1141
Versión de la política 1142
Documento de política JSON 1142
Más información 1143
AmazonS3OutpostsReadOnlyAccess 1143
Uso de la política 1143
Información de la política 1143
Versión de la política 1143
Documento de política JSON 1144
Más información 1145
AmazonS3ReadOnlyAccess 1145
Uso de la política 1145
Información de la política 1145
Versión de la política 1145
Documento de política JSON 1146
Más información 1146
AmazonS3TablesFullAccess 1146
Uso de la política 1147
Información de la política 1147
Versión de la política 1147
Documento de política JSON 1147
Más información 1147

AmazonS3TablesLakeFormationServiceRole 1148
Uso de la política 1148
Información de la política 1148
Versión de la política 1148
Documento de política JSON 1148
Más información 1151
AmazonS3TablesReadOnlyAccess 1151
Uso de la política 1151
Información de la política 1151
Versión de la política 1151
Documento de política JSON 1151
Más información 1152
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1152
Uso de la política 1152
Información de la política 1153
Versión de la política 1153
Documento de política JSON 1153
Más información 1164
AmazonSageMakerCanvasAIServicesAccess 1165
Uso de la política 1165
Información de la política 1165
Versión de la política 1165
Documento de política JSON 1165
Más información 1168
AmazonSageMakerCanvasBedrockAccess 1169
Uso de la política 1169
Información de la política 1169
Versión de la política 1169
Documento de política JSON 1169
Más información 1170
AmazonSageMakerCanvasDataPrepFullAccess 1170
Uso de la política 1170
Información de la política 1171
Versión de la política 1171
Documento de política JSON 1171
Más información 1180

AmazonSageMakerCanvasDirectDeployAccess 1181
Uso de la política 1181
Información de la política 1181
Versión de la política 1181
Documento de política JSON 1181
Más información 1182
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1182
Uso de la política 1183
Información de la política 1183
Versión de la política 1183
Documento de política JSON 1183
Más información 1184
AmazonSageMakerCanvasForecastAccess 1185
Uso de la política 1185
Información de la política 1185
Versión de la política 1185
Documento de política JSON 1185
Más información 1186
AmazonSageMakerCanvasFullAccess 1186
Uso de la política 1187
Información de la política 1187
Versión de la política 1187
Documento de política JSON 1187
Más información 1199
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1200
Uso de la política 1200
Información de la política 1200
Versión de la política 1200
Documento de política JSON 1200
Más información 1201
AmazonSageMakerClusterInstanceRolePolicy 1201
Uso de la política 1202
Información de la política 1202
Versión de la política 1202
Documento de política JSON 1202
Más información 1204

AmazonSageMakerCoreServiceRolePolicy 1204
Uso de la política 1204
Información de la política 1204
Versión de la política 1205
Documento de política JSON 1205
Más información 1206
AmazonSageMakerEdgeDeviceFleetPolicy 1206
Uso de la política 1206
Información de la política 1206
Versión de la política 1206
Documento de política JSON 1207
Más información 1208
AmazonSageMakerFeatureStoreAccess 1209
Uso de la política 1209
Información de la política 1209
Versión de la política 1209
Documento de política JSON 1209
Más información 1210
AmazonSageMakerFullAccess 1211
Uso de la política 1211
Información de la política 1211
Versión de la política 1211
Documento de política JSON 1211
Más información 1228
AmazonSageMakerGeospatialExecutionRole 1228
Uso de la política 1228
Información de la política 1228
Versión de la política 1228
Documento de política JSON 1229
Más información 1229
AmazonSageMakerGeospatialFullAccess 1230
Uso de la política 1230
Información de la política 1230
Versión de la política 1230
Documento de política JSON 1230
Más información 1231

AmazonSageMakerGroundTruthExecution 1231
Uso de la política 1231
Información de la política 1231
Versión de la política 1232
Documento de política JSON 1232
Más información 1235
AmazonSageMakerHyperPodObservabilityAdminAccess 1236
Uso de la política 1236
Información de la política 1236
Versión de la política 1236
Documento de política JSON 1236
Más información 1242
AmazonSageMakerHyperPodServiceRolePolicy 1243
Uso de la política 1243
Información de la política 1243
Versión de la política 1243
Documento de política JSON 1243
Más información 1244
AmazonSageMakerMechanicalTurkAccess 1245
Uso de la política 1245
Información de la política 1245
Versión de la política 1245
Documento de política JSON 1245
Más información 1246
AmazonSageMakerModelGovernanceUseAccess 1246
Uso de la política 1246
Información de la política 1246
Versión de la política 1246
Documento de política JSON 1247
Más información 1249
AmazonSageMakerModelRegistryFullAccess 1249
Uso de la política 1249
Información de la política 1249
Versión de la política 1249
Documento de política JSON 1250
Más información 1253

AmazonSageMakerNotebooksServiceRolePolicy 1253
Uso de la política 1254
Información de la política 1254
Versión de la política 1254
Documento de política JSON 1254
Más información 1258
AmazonSageMakerPartnerAppsFullAccess 1259
Uso de la política 1259
Información de la política 1259
Versión de la política 1259
Documento de política JSON 1259
Más información 1260
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1260
Uso de la política 1261
Información de la política 1261
Versión de la política 1261
Documento de política JSON 1261
Más información 1262
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1262
Uso de la política 1263
Información de la política 1263
Versión de la política 1263
Documento de política JSON 1263
Más información 1267
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1267
Uso de la política 1267
Información de la política 1267
Versión de la política 1267
Documento de política JSON 1268
Más información 1268
AmazonSageMakerPipelinesIntegrations 1268
Uso de la política 1269
Información de la política 1269
Versión de la política 1269
Documento de política JSON 1269
Más información 1271

AmazonSageMakerQuickSightVPCPolicy 1271
Uso de la política 1271
Información de la política 1272
Versión de la política 1272
Documento de política JSON 1272
Más información 1273
AmazonSageMakerReadOnly 1274
Uso de la política 1274
Información de la política 1274
Versión de la política 1274
Documento de política JSON 1274
Más información 1276
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1276
Uso de la política 1276
Información de la política 1276
Versión de la política 1276
Documento de política JSON 1277
Más información 1277
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1278
Uso de la política 1278
Información de la política 1278
Versión de la política 1278
Documento de política JSON 1279
Más información 1285
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1286
Uso de la política 1286
Información de la política 1286
Versión de la política 1286
Documento de política JSON 1286
Más información 1296
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1297
Uso de la política 1297
Información de la política 1297
Versión de la política 1297
Documento de política JSON 1297
Más información 1300

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1301
Uso de la política 1301
Información de la política 1301
Versión de la política 1301
Documento de política JSON 1301
Más información 1302
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1302
Uso de la política 1302
Información de la política 1302
Versión de la política 1303
Documento de política JSON 1303
Más información 1303
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1303
Uso de la política 1304
Información de la política 1304
Versión de la política 1304
Documento de política JSON 1304
Más información 1306
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1307
Uso de la política 1307
Información de la política 1307
Versión de la política 1307
Documento de política JSON 1307
Más información 1317
AmazonSageMakerTrainingPlanCreateAccess 1318
Uso de la política 1318
Información de la política 1318
Versión de la política 1318
Documento de política JSON 1318
Más información 1320
AmazonSecurityLakeAdministrator 1320
Uso de la política 1320
Información de la política 1320
Versión de la política 1320
Documento de política JSON 1321
Más información 1332

AmazonSecurityLakeMetastoreManager 1332
Uso de la política 1332
Información de la política 1332
Versión de la política 1332
Documento de política JSON 1333
Más información 1335
AmazonSecurityLakePermissionsBoundary 1335
Uso de la política 1335
Información de la política 1335
Versión de la política 1336
Documento de política JSON 1336
Más información 1339
AmazonSESFullAccess 1339
Uso de la política 1339
Información de la política 1339
Versión de la política 1340
Documento de política JSON 1340
Más información 1340
AmazonSESReadOnlyAccess 1341
Uso de la política 1341
Información de la política 1341
Versión de la política 1341
Documento de política JSON 1341
Más información 1342
AmazonSESServiceRolePolicy 1342
Uso de la política 1342
Información de la política 1342
Versión de la política 1342
Documento de política JSON 1343
Más información 1343
AmazonSNSFullAccess 1343
Uso de la política 1344
Información de la política 1344
Versión de la política 1344
Documento de política JSON 1344
Más información 1345

AmazonSNSReadOnlyAccess 1345
Uso de la política 1345
Información de la política 1345
Versión de la política 1346
Documento de política JSON 1346
Más información 1347
AmazonSNSRole 1347
Uso de la política 1347
Información de la política 1347
Versión de la política 1348
Documento de política JSON 1348
Más información 1348
AmazonSQSFullAccess 1349
Uso de la política 1349
Información de la política 1349
Versión de la política 1349
Documento de política JSON 1349
Más información 1350
AmazonSQSReadOnlyAccess 1350
Uso de la política 1350
Información de la política 1350
Versión de la política 1350
Documento de política JSON 1351
Más información 1351
AmazonSSMAutomationApproverAccess 1351
Uso de la política 1352
Información de la política 1352
Versión de la política 1352
Documento de política JSON 1352
Más información 1353
AmazonSSMAutomationRole 1353
Uso de la política 1353
Información de la política 1353
Versión de la política 1353
Documento de política JSON 1354
Más información 1355

AmazonSSMDirectoryServiceAccess 1355
Uso de la política 1355
Información de la política 1356
Versión de la política 1356
Documento de política JSON 1356
Más información 1356
AmazonSSMFullAccess 1357
Uso de la política 1357
Información de la política 1357
Versión de la política 1357
Documento de política JSON 1357
Más información 1359
AmazonSSMMaintenanceWindowRole 1359
Uso de la política 1359
Información de la política 1359
Versión de la política 1359
Documento de política JSON 1359
Más información 1361
AmazonSSMManagedEC2InstanceDefaultPolicy 1361
Uso de la política 1361
Información de la política 1361
Versión de la política 1362
Documento de política JSON 1362
Más información 1363
AmazonSSMManagedInstanceCore 1363
Uso de la política 1363
Información de la política 1363
Versión de la política 1364
Documento de política JSON 1364
Más información 1365
AmazonSSMPatchAssociation 1365
Uso de la política 1366
Información de la política 1366
Versión de la política 1366
Documento de política JSON 1366
Más información 1367

AmazonSSMReadOnlyAccess 1367
Uso de la política 1367
Información de la política 1367
Versión de la política 1367
Documento de política JSON 1368
Más información 1368
AmazonSSMServiceRolePolicy 1368
Uso de la política 1369
Información de la política 1369
Versión de la política 1369
Documento de política JSON 1369
Más información 1374
AmazonSumerianFullAccess 1374
Uso de la política 1375
Información de la política 1375
Versión de la política 1375
Documento de política JSON 1375
Más información 1375
AmazonTextractFullAccess 1376
Uso de la política 1376
Información de la política 1376
Versión de la política 1376
Documento de política JSON 1376
Más información 1377
AmazonTextractServiceRole 1377
Uso de la política 1377
Información de la política 1377
Versión de la política 1377
Documento de política JSON 1378
Más información 1378
AmazonTimestreamConsoleFullAccess 1378
Uso de la política 1379
Información de la política 1379
Versión de la política 1379
Documento de política JSON 1379
Más información 1381

AmazonTimestreamFullAccess 1381
Uso de la política 1381
Información de la política 1382
Versión de la política 1382
Documento de política JSON 1382
Más información 1383
AmazonTimestreamInfluxDBFullAccess 1383
Uso de la política 1384
Información de la política 1384
Versión de la política 1384
Documento de política JSON 1384
Más información 1387
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1387
Uso de la política 1387
Información de la política 1387
Versión de la política 1388
Documento de política JSON 1388
Más información 1390
AmazonTimestreamInfluxDBServiceRolePolicy 1390
Uso de la política 1390
Información de la política 1390
Versión de la política 1391
Documento de política JSON 1391
Más información 1393
AmazonTimestreamReadOnlyAccess 1393
Uso de la política 1394
Información de la política 1394
Versión de la política 1394
Documento de política JSON 1394
Más información 1395
AmazonTranscribeFullAccess 1395
Uso de la política 1395
Información de la política 1395
Versión de la política 1396
Documento de política JSON 1396
Más información 1396

AmazonTranscribeReadOnlyAccess 1397
Uso de la política 1397
Información de la política 1397
Versión de la política 1397
Documento de política JSON 1397
Más información 1398
AmazonVerifiedPermissionsFullAccess 1398
Uso de la política 1398
Información de la política 1398
Versión de la política 1398
Documento de política JSON 1399
Más información 1399
AmazonVerifiedPermissionsReadOnlyAccess 1399
Uso de la política 1400
Información de la política 1400
Versión de la política 1400
Documento de política JSON 1400
Más información 1401
AmazonVPCCrossAccountNetworkInterfaceOperations 1401
Uso de la política 1401
Información de la política 1401
Versión de la política 1402
Documento de política JSON 1402
Más información 1403
AmazonVPCFullAccess 1404
Uso de la política 1404
Información de la política 1404
Versión de la política 1404
Documento de política JSON 1404
Más información 1408
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1408
Uso de la política 1409
Información de la política 1409
Versión de la política 1409
Documento de política JSON 1409
Más información 1412

AmazonVPCReachabilityAnalyzerFullAccessPolicy 1413
Uso de la política 1413
Información de la política 1413
Versión de la política 1413
Documento de política JSON 1413
Más información 1416
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1417
Uso de la política 1417
Información de la política 1417
Versión de la política 1417
Documento de política JSON 1417
Más información 1418
AmazonVPCReadOnlyAccess 1418
Uso de la política 1418
Información de la política 1418
Versión de la política 1419
Documento de política JSON 1419
Más información 1420
AmazonWorkDocsFullAccess 1420
Uso de la política 1421
Información de la política 1421
Versión de la política 1421
Documento de política JSON 1421
Más información 1422
AmazonWorkDocsReadOnlyAccess 1422
Uso de la política 1422
Información de la política 1422
Versión de la política 1422
Documento de política JSON 1423
Más información 1423
AmazonWorkMailEventsServiceRolePolicy 1423
Uso de la política 1423
Información de la política 1424
Versión de la política 1424
Documento de política JSON 1424
Más información 1424

AmazonWorkMailFullAccess 1425
Uso de la política 1425
Información de la política 1425
Versión de la política 1425
Documento de política JSON 1425
Más información 1427
AmazonWorkMailMessageFlowFullAccess 1427
Uso de la política 1428
Información de la política 1428
Versión de la política 1428
Documento de política JSON 1428
Más información 1429
AmazonWorkMailMessageFlowReadOnlyAccess 1429
Uso de la política 1429
Información de la política 1429
Versión de la política 1429
Documento de política JSON 1429
Más información 1430
AmazonWorkMailReadOnlyAccess 1430
Uso de la política 1430
Información de la política 1430
Versión de la política 1431
Documento de política JSON 1431
Más información 1431
AmazonWorkSpacesAdmin 1432
Uso de la política 1432
Información de la política 1432
Versión de la política 1432
Documento de política JSON 1432
Más información 1433
AmazonWorkSpacesApplicationManagerAdminAccess 1434
Uso de la política 1434
Información de la política 1434
Versión de la política 1434
Documento de política JSON 1434
Más información 1435

AmazonWorkspacesPCAAccess 1435
Uso de la política 1435
Información de la política 1435
Versión de la política 1435
Documento de política JSON 1436
Más información 1436
AmazonWorkSpacesPoolServiceAccess 1436
Uso de la política 1437
Información de la política 1437
Versión de la política 1437
Documento de política JSON 1437
Más información 1438
AmazonWorkSpacesSecureBrowserReadOnly 1439
Uso de la política 1439
Información de la política 1439
Versión de la política 1439
Documento de política JSON 1439
Más información 1440
AmazonWorkSpacesSelfServiceAccess 1441
Uso de la política 1441
Información de la política 1441
Versión de la política 1441
Documento de política JSON 1441
Más información 1442
AmazonWorkSpacesServiceAccess 1442
Uso de la política 1442
Información de la política 1442
Versión de la política 1442
Documento de política JSON 1443
Más información 1443
AmazonWorkSpacesThinClientFullAccess 1443
Uso de la política 1443
Información de la política 1444
Versión de la política 1444
Documento de política JSON 1444
Más información 1445

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1445
Uso de la política 1445
Información de la política 1446
Versión de la política 1446
Documento de política JSON 1446
Más información 1447
AmazonWorkSpacesThinClientReadOnlyAccess 1447
Uso de la política 1447
Información de la política 1447
Versión de la política 1447
Documento de política JSON 1447
Más información 1449
AmazonWorkSpacesWebReadOnly 1449
Uso de la política 1449
Información de la política 1449
Versión de la política 1449
Documento de política JSON 1450
Más información 1451
AmazonWorkSpacesWebServiceRolePolicy 1451
Uso de la política 1451
Información de la política 1451
Versión de la política 1451
Documento de política JSON 1452
Más información 1454
AmazonZocaloFullAccess 1454
Uso de la política 1454
Información de la política 1454
Versión de la política 1454
Documento de política JSON 1455
Más información 1455
AmazonZocaloReadOnlyAccess 1456
Uso de la política 1456
Información de la política 1456
Versión de la política 1456
Documento de política JSON 1456
Más información 1457

AmplifyBackendDeployFullAccess 1457
Uso de la política 1457
Información de la política 1457
Versión de la política 1458
Documento de política JSON 1458
Más información 1462
APIGatewayServiceRolePolicy 1462
Uso de la política 1462
Información de la política 1463
Versión de la política 1463
Documento de política JSON 1463
Más información 1465
AppIntegrationsServiceLinkedRolePolicy 1465
Uso de la política 1466
Información de la política 1466
Versión de la política 1466
Documento de política JSON 1466
Más información 1468
ApplicationAutoScalingForAmazonAppStreamAccess 1468
Uso de la política 1468
Información de la política 1468
Versión de la política 1468
Documento de política JSON 1469
Más información 1469
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1470
Uso de la política 1470
Información de la política 1470
Versión de la política 1470
Documento de política JSON 1470
Más información 1472
AppRunnerNetworkingServiceRolePolicy 1472
Uso de la política 1473
Información de la política 1473
Versión de la política 1473
Documento de política JSON 1473
Más información 1474

AppRunnerServiceRolePolicy 1475
Uso de la política 1475
Información de la política 1475
Versión de la política 1475
Documento de política JSON 1475
Más información 1476
AppStudioServiceRolePolicy 1476
Uso de la política 1477
Información de la política 1477
Versión de la política 1477
Documento de política JSON 1477
Más información 1479
AuroraDsqlServiceLinkedRolePolicy 1479
Uso de la política 1480
Información de la política 1480
Versión de la política 1480
Documento de política JSON 1480
Más información 1481
AutoScalingConsoleFullAccess 1481
Uso de la política 1481
Información de la política 1481
Versión de la política 1481
Documento de política JSON 1482
Más información 1483
AutoScalingConsoleReadOnlyAccess 1484
Uso de la política 1484
Información de la política 1484
Versión de la política 1484
Documento de política JSON 1484
Más información 1485
AutoScalingFullAccess 1486
Uso de la política 1486
Información de la política 1486
Versión de la política 1486
Documento de política JSON 1486
Más información 1487

AutoScalingNotificationAccessRole 1488
Uso de la política 1488
Información de la política 1488
Versión de la política 1488
Documento de política JSON 1488
Más información 1489
AutoScalingReadOnlyAccess 1489
Uso de la política 1489
Información de la política 1489
Versión de la política 1490
Documento de política JSON 1490
Más información 1490
AutoScalingServiceRolePolicy 1490
Uso de la política 1491
Información de la política 1491
Versión de la política 1491
Documento de política JSON 1491
Más información 1494
AWS-SSM-Automation-DiagnosisBucketPolicy 1494
Uso de la política 1494
Información de la política 1495
Versión de la política 1495
Documento de política JSON 1495
Más información 1497
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1498
Uso de la política 1498
Información de la política 1498
Versión de la política 1498
Documento de política JSON 1498
Más información 1501
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1501
Uso de la política 1501
Información de la política 1501
Versión de la política 1502
Documento de política JSON 1502
Más información 1504

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1504
Uso de la política 1504
Información de la política 1504
Versión de la política 1505
Documento de política JSON 1505
Más información 1505
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1506
Uso de la política 1506
Información de la política 1506
Versión de la política 1506
Documento de política JSON 1507
Más información 1509
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1509
Uso de la política 1510
Información de la política 1510
Versión de la política 1510
Documento de política JSON 1510
Más información 1516
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1517
Uso de la política 1517
Información de la política 1517
Versión de la política 1517
Documento de política JSON 1517
Más información 1518
AWS_ConfigRole 1518
Uso de la política 1519
Información de la política 1519
Versión de la política 1519
Documento de política JSON 1519
Más información 1556
AWSAccountActivityAccess 1556
Uso de la política 1556
Información de la política 1556
Versión de la política 1557
Documento de política JSON 1557
Más información 1558

AWSAccountManagementFullAccess 1558
Uso de la política 1558
Información de la política 1558
Versión de la política 1558
Documento de política JSON 1558
Más información 1559
AWSAccountManagementReadOnlyAccess 1559
Uso de la política 1559
Información de la política 1559
Versión de la política 1560
Documento de política JSON 1560
Más información 1560
AWSAccountUsageReportAccess 1560
Uso de la política 1561
Información de la política 1561
Versión de la política 1561
Documento de política JSON 1561
Más información 1561
AWSAgentlessDiscoveryService 1562
Uso de la política 1562
Información de la política 1562
Versión de la política 1562
Documento de política JSON 1562
Más información 1564
AWSAppFabricFullAccess 1564
Uso de la política 1565
Información de la política 1565
Versión de la política 1565
Documento de política JSON 1565
Más información 1566
AWSAppFabricReadOnlyAccess 1567
Uso de la política 1567
Información de la política 1567
Versión de la política 1567
Documento de política JSON 1567
Más información 1568

AWSAppFabricServiceRolePolicy 1568
Uso de la política 1568
Información de la política 1568
Versión de la política 1569
Documento de política JSON 1569
Más información 1570
AWSApplicationAutoscalingAppStreamFleetPolicy 1570
Uso de la política 1570
Información de la política 1570
Versión de la política 1571
Documento de política JSON 1571
Más información 1571
AWSApplicationAutoscalingCassandraTablePolicy 1572
Uso de la política 1572
Información de la política 1572
Versión de la política 1572
Documento de política JSON 1572
Más información 1573
AWSApplicationAutoscalingComprehendEndpointPolicy 1573
Uso de la política 1573
Información de la política 1573
Versión de la política 1574
Documento de política JSON 1574
Más información 1574
AWSApplicationAutoScalingCustomResourcePolicy 1575
Uso de la política 1575
Información de la política 1575
Versión de la política 1575
Documento de política JSON 1575
Más información 1576
AWSApplicationAutoscalingDynamoDBTablePolicy 1576
Uso de la política 1576
Información de la política 1576
Versión de la política 1576
Documento de política JSON 1577
Más información 1577

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1577
Uso de la política 1578
Información de la política 1578
Versión de la política 1578
Documento de política JSON 1578
Más información 1579
AWSApplicationAutoscalingECSServicePolicy 1579
Uso de la política 1579
Información de la política 1579
Versión de la política 1579
Documento de política JSON 1580
Más información 1580
AWSApplicationAutoscalingElastiCacheRGPolicy 1580
Uso de la política 1580
Información de la política 1581
Versión de la política 1581
Documento de política JSON 1581
Más información 1582
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1582
Uso de la política 1582
Información de la política 1583
Versión de la política 1583
Documento de política JSON 1583
Más información 1583
AWSApplicationAutoscalingKafkaClusterPolicy 1584
Uso de la política 1584
Información de la política 1584
Versión de la política 1584
Documento de política JSON 1584
Más información 1585
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1585
Uso de la política 1585
Información de la política 1585
Versión de la política 1586
Documento de política JSON 1586
Más información 1586

AWSApplicationAutoscalingNeptuneClusterPolicy 1587
Uso de la política 1587
Información de la política 1587
Versión de la política 1587
Documento de política JSON 1587
Más información 1589
AWSApplicationAutoscalingRDSClusterPolicy 1589
Uso de la política 1589
Información de la política 1589
Versión de la política 1589
Documento de política JSON 1590
Más información 1590
AWSApplicationAutoscalingSageMakerEndpointPolicy 1591
Uso de la política 1591
Información de la política 1591
Versión de la política 1591
Documento de política JSON 1591
Más información 1592
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1592
Uso de la política 1593
Información de la política 1593
Versión de la política 1593
Documento de política JSON 1593
Más información 1594
AWSApplicationDiscoveryAgentAccess 1595
Uso de la política 1595
Información de la política 1595
Versión de la política 1595
Documento de política JSON 1595
Más información 1596
AWSApplicationDiscoveryAgentlessCollectorAccess 1596
Uso de la política 1596
Información de la política 1596
Versión de la política 1597
Documento de política JSON 1597
Más información 1598

AWSApplicationDiscoveryServiceFullAccess 1598
Uso de la política 1598
Información de la política 1598
Versión de la política 1599
Documento de política JSON 1599
Más información 1600
AWSApplicationMigrationAgentInstallationPolicy 1600
Uso de la política 1601
Información de la política 1601
Versión de la política 1601
Documento de política JSON 1601
Más información 1602
AWSApplicationMigrationAgentPolicy 1602
Uso de la política 1603
Información de la política 1603
Versión de la política 1603
Documento de política JSON 1603
Más información 1604
AWSApplicationMigrationAgentPolicy_v2 1604
Uso de la política 1604
Información de la política 1605
Versión de la política 1605
Documento de política JSON 1605
Más información 1606
AWSApplicationMigrationConversionServerPolicy 1606
Uso de la política 1606
Información de la política 1606
Versión de la política 1607
Documento de política JSON 1607
Más información 1607
AWSApplicationMigrationEC2Access 1608
Uso de la política 1608
Información de la política 1608
Versión de la política 1608
Documento de política JSON 1608
Más información 1616

AWSApplicationMigrationFullAccess 1617
Uso de la política 1617
Información de la política 1617
Versión de la política 1617
Documento de política JSON 1617
Más información 1623
AWSApplicationMigrationMGHAccess 1624
Uso de la política 1624
Información de la política 1624
Versión de la política 1624
Documento de política JSON 1624
Más información 1625
AWSApplicationMigrationReadOnlyAccess 1625
Uso de la política 1625
Información de la política 1625
Versión de la política 1626
Documento de política JSON 1626
Más información 1627
AWSApplicationMigrationReplicationServerPolicy 1627
Uso de la política 1628
Información de la política 1628
Versión de la política 1628
Documento de política JSON 1628
Más información 1630
AWSApplicationMigrationServiceEc2InstancePolicy 1630
Uso de la política 1630
Información de la política 1630
Versión de la política 1631
Documento de política JSON 1631
Más información 1632
AWSApplicationMigrationServiceRolePolicy 1632
Uso de la política 1632
Información de la política 1632
Versión de la política 1633
Documento de política JSON 1633
Más información 1640

AWSApplicationMigrationSSMAccess 1640
Uso de la política 1641
Información de la política 1641
Versión de la política 1641
Documento de política JSON 1641
Más información 1643
AWSApplicationMigrationVCenterClientPolicy 1643
Uso de la política 1643
Información de la política 1644
Versión de la política 1644
Documento de política JSON 1644
Más información 1645
AWSAppMeshEnvoyAccess 1645
Uso de la política 1645
Información de la política 1645
Versión de la política 1645
Documento de política JSON 1646
Más información 1646
AWSAppMeshFullAccess 1646
Uso de la política 1646
Información de la política 1646
Versión de la política 1647
Documento de política JSON 1647
Más información 1648
AWSAppMeshPreviewEnvoyAccess 1649
Uso de la política 1649
Información de la política 1649
Versión de la política 1649
Documento de política JSON 1649
Más información 1650
AWSAppMeshPreviewServiceRolePolicy 1650
Uso de la política 1650
Información de la política 1650
Versión de la política 1650
Documento de política JSON 1651
Más información 1651

AWSAppMeshReadOnly 1651
Uso de la política 1652
Información de la política 1652
Versión de la política 1652
Documento de política JSON 1652
Más información 1653
AWSAppMeshServiceRolePolicy 1653
Uso de la política 1654
Información de la política 1654
Versión de la política 1654
Documento de política JSON 1654
Más información 1655
AWSAppRunnerFullAccess 1655
Uso de la política 1655
Información de la política 1655
Versión de la política 1655
Documento de política JSON 1656
Más información 1656
AWSAppRunnerReadOnlyAccess 1657
Uso de la política 1657
Información de la política 1657
Versión de la política 1657
Documento de política JSON 1657
Más información 1658
AWSAppRunnerServicePolicyForECRAccess 1658
Uso de la política 1658
Información de la política 1658
Versión de la política 1658
Documento de política JSON 1659
Más información 1659
AWSAppSyncAdministrator 1659
Uso de la política 1660
Información de la política 1660
Versión de la política 1660
Documento de política JSON 1660
Más información 1661

AWSAppSyncInvokeFullAccess 1661
Uso de la política 1662
Información de la política 1662
Versión de la política 1662
Documento de política JSON 1662
Más información 1663
AWSAppSyncPushToCloudWatchLogs 1663
Uso de la política 1663
Información de la política 1663
Versión de la política 1663
Documento de política JSON 1663
Más información 1664
AWSAppSyncSchemaAuthor 1664
Uso de la política 1664
Información de la política 1664
Versión de la política 1665
Documento de política JSON 1665
Más información 1666
AWSAppSyncServiceRolePolicy 1666
Uso de la política 1666
Información de la política 1666
Versión de la política 1667
Documento de política JSON 1667
Más información 1667
AWSArtifactAccountSync 1667
Uso de la política 1668
Información de la política 1668
Versión de la política 1668
Documento de política JSON 1668
Más información 1669
AWSArtifactAgreementsFullAccess 1669
Uso de la política 1669
Información de la política 1669
Versión de la política 1669
Documento de política JSON 1670
Más información 1671

AWSArtifactAgreementsReadOnlyAccess 1672
Uso de la política 1672
Información de la política 1672
Versión de la política 1672
Documento de política JSON 1672
Más información 1673
AWSArtifactReportsReadOnlyAccess 1674
Uso de la política 1674
Información de la política 1674
Versión de la política 1674
Documento de política JSON 1674
Más información 1675
AWSArtifactServiceRolePolicy 1675
Uso de la política 1675
Información de la política 1675
Versión de la política 1675
Documento de política JSON 1676
Más información 1676
AWSAuditManagerAdministratorAccess 1676
Uso de la política 1676
Información de la política 1677
Versión de la política 1677
Documento de política JSON 1677
Más información 1681
AWSAuditManagerServiceRolePolicy 1681
Uso de la política 1681
Información de la política 1681
Versión de la política 1682
Documento de política JSON 1682
Más información 1689
AWSAutoScalingPlansEC2AutoScalingPolicy 1689
Uso de la política 1689
Información de la política 1689
Versión de la política 1689
Documento de política JSON 1690
Más información 1690

AWSBackupAuditAccess 1690
Uso de la política 1691
Información de la política 1691
Versión de la política 1691
Documento de política JSON 1691
Más información 1692
AWSBackupDataTransferAccess 1693
Uso de la política 1693
Información de la política 1693
Versión de la política 1693
Documento de política JSON 1693
Más información 1694
AWSBackupFullAccess 1694
Uso de la política 1694
Información de la política 1694
Versión de la política 1695
Documento de política JSON 1695
Más información 1706
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1706
Uso de la política 1706
Información de la política 1706
Versión de la política 1707
Documento de política JSON 1707
Más información 1708
AWSBackupOperatorAccess 1708
Uso de la política 1708
Información de la política 1708
Versión de la política 1708
Documento de política JSON 1709
Más información 1717
AWSBackupOrganizationAdminAccess 1717
Uso de la política 1717
Información de la política 1718
Versión de la política 1718
Documento de política JSON 1718
Más información 1720

AWSBackupRestoreAccessForSAPHANA 1720
Uso de la política 1720
Información de la política 1720
Versión de la política 1721
Documento de política JSON 1721
Más información 1722
AWSBackupSearchOperatorAccess 1722
Uso de la política 1722
Información de la política 1722
Versión de la política 1722
Documento de política JSON 1723
Más información 1724
AWSBackupServiceLinkedRolePolicyForBackup 1725
Uso de la política 1725
Información de la política 1725
Versión de la política 1725
Documento de política JSON 1725
Más información 1735
AWSBackupServiceLinkedRolePolicyForBackupTest 1735
Uso de la política 1735
Información de la política 1735
Versión de la política 1735
Documento de política JSON 1735
Más información 1736
AWSBackupServiceRolePolicyForBackup 1736
Uso de la política 1736
Información de la política 1737
Versión de la política 1737
Documento de política JSON 1737
Más información 1750
AWSBackupServiceRolePolicyForIndexing 1751
Uso de la política 1751
Información de la política 1751
Versión de la política 1751
Documento de política JSON 1751
Más información 1752

AWSBackupServiceRolePolicyForItemRestores 1753
Uso de la política 1753
Información de la política 1753
Versión de la política 1753
Documento de política JSON 1753
Más información 1755
AWSBackupServiceRolePolicyForRestores 1755
Uso de la política 1755
Información de la política 1756
Versión de la política 1756
Documento de política JSON 1756
Más información 1767
AWSBackupServiceRolePolicyForS3Backup 1768
Uso de la política 1768
Información de la política 1768
Versión de la política 1768
Documento de política JSON 1768
Más información 1771
AWSBackupServiceRolePolicyForS3Restore 1771
Uso de la política 1771
Información de la política 1771
Versión de la política 1771
Documento de política JSON 1772
Más información 1773
AWSBatchFullAccess 1773
Uso de la política 1773
Información de la política 1773
Versión de la política 1774
Documento de política JSON 1774
Más información 1775
AWSBatchServiceEventTargetRole 1775
Uso de la política 1776
Información de la política 1776
Versión de la política 1776
Documento de política JSON 1776
Más información 1776

AWSBatchServiceRole 1777
Uso de la política 1777
Información de la política 1777
Versión de la política 1777
Documento de política JSON 1777
Más información 1780
AWSBCMDataExportsServiceRolePolicy 1781
Uso de la política 1781
Información de la política 1781
Versión de la política 1781
Documento de política JSON 1781
Más información 1782
AWSBillingConductorFullAccess 1782
Uso de la política 1782
Información de la política 1782
Versión de la política 1783
Documento de política JSON 1783
Más información 1783
AWSBillingConductorReadOnlyAccess 1783
Uso de la política 1784
Información de la política 1784
Versión de la política 1784
Documento de política JSON 1784
Más información 1785
AWSBillingReadOnlyAccess 1785
Uso de la política 1785
Información de la política 1785
Versión de la política 1785
Documento de política JSON 1786
Más información 1787
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1788
Uso de la política 1788
Información de la política 1788
Versión de la política 1788
Documento de política JSON 1788
Más información 1789

AWSBudgetsActionsWithAWSResourceControlAccess 1790
Uso de la política 1790
Información de la política 1790
Versión de la política 1790
Documento de política JSON 1790
Más información 1792
AWSBudgetsReadOnlyAccess 1792
Uso de la política 1792
Información de la política 1792
Versión de la política 1792
Documento de política JSON 1793
Más información 1793
AWSBugBustFullAccess 1793
Uso de la política 1793
Información de la política 1794
Versión de la política 1794
Documento de política JSON 1794
Más información 1795
AWSBugBustPlayerAccess 1795
Uso de la política 1796
Información de la política 1796
Versión de la política 1796
Documento de política JSON 1796
Más información 1797
AWSBugBustServiceRolePolicy 1797
Uso de la política 1797
Información de la política 1798
Versión de la política 1798
Documento de política JSON 1798
Más información 1798
AWSCertificateManagerFullAccess 1799
Uso de la política 1799
Información de la política 1799
Versión de la política 1799
Documento de política JSON 1799
Más información 1800

AWSCertificateManagerPrivateCAAuditor 1800
Uso de la política 1801
Información de la política 1801
Versión de la política 1801
Documento de política JSON 1801
Más información 1802
AWSCertificateManagerPrivateCAFullAccess 1802
Uso de la política 1802
Información de la política 1802
Versión de la política 1803
Documento de política JSON 1803
Más información 1803
AWSCertificateManagerPrivateCAPrivilegedUser 1803
Uso de la política 1804
Información de la política 1804
Versión de la política 1804
Documento de política JSON 1804
Más información 1805
AWSCertificateManagerPrivateCAReadOnly 1806
Uso de la política 1806
Información de la política 1806
Versión de la política 1806
Documento de política JSON 1806
Más información 1807
AWSCertificateManagerPrivateCAUser 1807
Uso de la política 1807
Información de la política 1807
Versión de la política 1807
Documento de política JSON 1808
Más información 1809
AWSCertificateManagerReadOnly 1809
Uso de la política 1809
Información de la política 1809
Versión de la política 1810
Documento de política JSON 1810
Más información 1810

AWSChatbotServiceLinkedRolePolicy 1810
Uso de la política 1811
Información de la política 1811
Versión de la política 1811
Documento de política JSON 1811
Más información 1812
AWSCleanRoomsFullAccess 1812
Uso de la política 1812
Información de la política 1812
Versión de la política 1812
Documento de política JSON 1813
Más información 1817
AWSCleanRoomsFullAccessNoQuerying 1817
Uso de la política 1817
Información de la política 1818
Versión de la política 1818
Documento de política JSON 1818
Más información 1823
AWSCleanRoomsMLFullAccess 1823
Uso de la política 1823
Información de la política 1823
Versión de la política 1823
Documento de política JSON 1824
Más información 1828
AWSCleanRoomsMLReadOnlyAccess 1828
Uso de la política 1828
Información de la política 1828
Versión de la política 1828
Documento de política JSON 1829
Más información 1830
AWSCleanRoomsReadOnlyAccess 1830
Uso de la política 1830
Información de la política 1830
Versión de la política 1830
Documento de política JSON 1831
Más información 1832

AWSCloud9Administrator 1832
Uso de la política 1832
Información de la política 1832
Versión de la política 1833
Documento de política JSON 1833
Más información 1834
AWSCloud9EnvironmentMember 1834
Uso de la política 1835
Información de la política 1835
Versión de la política 1835
Documento de política JSON 1835
Más información 1836
AWSCloud9ServiceRolePolicy 1837
Uso de la política 1837
Información de la política 1837
Versión de la política 1837
Documento de política JSON 1837
Más información 1840
AWSCloud9SSMInstanceProfile 1840
Uso de la política 1840
Información de la política 1840
Versión de la política 1840
Documento de política JSON 1841
Más información 1841
AWSCloud9User 1841
Uso de la política 1842
Información de la política 1842
Versión de la política 1842
Documento de política JSON 1842
Más información 1844
AWSCloudFormationFullAccess 1845
Uso de la política 1845
Información de la política 1845
Versión de la política 1845
Documento de política JSON 1845
Más información 1846

AWSCloudFormationReadOnlyAccess 1846
Uso de la política 1846
Información de la política 1846
Versión de la política 1846
Documento de política JSON 1847
Más información 1847
AWSCloudFrontLogger 1847
Uso de la política 1847
Información de la política 1848
Versión de la política 1848
Documento de política JSON 1848
Más información 1848
AWSCloudFrontVPCOriginServiceRolePolicy 1849
Uso de la política 1849
Información de la política 1849
Versión de la política 1849
Documento de política JSON 1849
Más información 1852
AWSCloudHSMFullAccess 1852
Uso de la política 1852
Información de la política 1852
Versión de la política 1853
Documento de política JSON 1853
Más información 1853
AWSCloudHSMReadOnlyAccess 1853
Uso de la política 1853
Información de la política 1854
Versión de la política 1854
Documento de política JSON 1854
Más información 1854
AWSCloudHSMRole 1855
Uso de la política 1855
Información de la política 1855
Versión de la política 1855
Documento de política JSON 1855
Más información 1856

AWSCloudMapDiscoverInstanceAccess 1856
Uso de la política 1856
Información de la política 1856
Versión de la política 1857
Documento de política JSON 1857
Más información 1857
AWSCloudMapFullAccess 1857
Uso de la política 1858
Información de la política 1858
Versión de la política 1858
Documento de política JSON 1858
Más información 1859
AWSCloudMapReadOnlyAccess 1859
Uso de la política 1859
Información de la política 1859
Versión de la política 1860
Documento de política JSON 1860
Más información 1860
AWSCloudMapRegisterInstanceAccess 1861
Uso de la política 1861
Información de la política 1861
Versión de la política 1861
Documento de política JSON 1861
Más información 1862
AWSCloudShellFullAccess 1862
Uso de la política 1862
Información de la política 1862
Versión de la política 1863
Documento de política JSON 1863
Más información 1863
AWSCloudTrail_FullAccess 1863
Uso de la política 1864
Información de la política 1864
Versión de la política 1864
Documento de política JSON 1864
Más información 1867

AWSCloudTrail_ReadOnlyAccess 1867
Uso de la política 1867
Información de la política 1867
Versión de la política 1867
Documento de política JSON 1867
Más información 1868
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1868
Uso de la política 1868
Información de la política 1869
Versión de la política 1869
Documento de política JSON 1869
Más información 1869
AWSCodeArtifactAdminAccess 1870
Uso de la política 1870
Información de la política 1870
Versión de la política 1870
Documento de política JSON 1870
Más información 1871
AWSCodeArtifactReadOnlyAccess 1871
Uso de la política 1871
Información de la política 1871
Versión de la política 1872
Documento de política JSON 1872
Más información 1872
AWSCodeBuildAdminAccess 1873
Uso de la política 1873
Información de la política 1873
Versión de la política 1873
Documento de política JSON 1873
Más información 1877
AWSCodeBuildDeveloperAccess 1877
Uso de la política 1877
Información de la política 1877
Versión de la política 1877
Documento de política JSON 1878
Más información 1880

AWSCodeBuildReadOnlyAccess 1881
Uso de la política 1881
Información de la política 1881
Versión de la política 1881
Documento de política JSON 1881
Más información 1883
AWSCodeCommitFullAccess 1883
Uso de la política 1883
Información de la política 1883
Versión de la política 1883
Documento de política JSON 1884
Más información 1888
AWSCodeCommitPowerUser 1889
Uso de la política 1889
Información de la política 1889
Versión de la política 1889
Documento de política JSON 1889
Más información 1894
AWSCodeCommitReadOnly 1894
Uso de la política 1894
Información de la política 1895
Versión de la política 1895
Documento de política JSON 1895
Más información 1898
AWSCodeDeployDeployerAccess 1898
Uso de la política 1898
Información de la política 1898
Versión de la política 1898
Documento de política JSON 1898
Más información 1900
AWSCodeDeployFullAccess 1900
Uso de la política 1900
Información de la política 1900
Versión de la política 1901
Documento de política JSON 1901
Más información 1902

AWSCodeDeployReadOnlyAccess 1903
Uso de la política 1903
Información de la política 1903
Versión de la política 1903
Documento de política JSON 1903
Más información 1904
AWSCodeDeployRole 1905
Uso de la política 1905
Información de la política 1905
Versión de la política 1905
Documento de política JSON 1905
Más información 1907
AWSCodeDeployRoleForCloudFormation 1907
Uso de la política 1907
Información de la política 1907
Versión de la política 1907
Documento de política JSON 1908
Más información 1908
AWSCodeDeployRoleForECS 1908
Uso de la política 1908
Información de la política 1909
Versión de la política 1909
Documento de política JSON 1909
Más información 1910
AWSCodeDeployRoleForECSLimited 1910
Uso de la política 1910
Información de la política 1910
Versión de la política 1911
Documento de política JSON 1911
Más información 1913
AWSCodeDeployRoleForLambda 1913
Uso de la política 1913
Información de la política 1913
Versión de la política 1913
Documento de política JSON 1914
Más información 1915

AWSCodeDeployRoleForLambdaLimited 1915
Uso de la política 1915
Información de la política 1915
Versión de la política 1915
Documento de política JSON 1916
Más información 1917
AWSCodePipeline_FullAccess 1917
Uso de la política 1917
Información de la política 1917
Versión de la política 1917
Documento de política JSON 1918
Más información 1921
AWSCodePipeline_ReadOnlyAccess 1922
Uso de la política 1922
Información de la política 1922
Versión de la política 1922
Documento de política JSON 1922
Más información 1923
AWSCodePipelineApproverAccess 1924
Uso de la política 1924
Información de la política 1924
Versión de la política 1924
Documento de política JSON 1924
Más información 1925
AWSCodePipelineCustomActionAccess 1925
Uso de la política 1925
Información de la política 1925
Versión de la política 1926
Documento de política JSON 1926
Más información 1926
AWSCodeStarFullAccess 1927
Uso de la política 1927
Información de la política 1927
Versión de la política 1927
Documento de política JSON 1927
Más información 1928

AWSCodeStarNotificationsServiceRolePolicy 1928
Uso de la política 1928
Información de la política 1929
Versión de la política 1929
Documento de política JSON 1929
Más información 1930
AWSCodeStarServiceRole 1930
Uso de la política 1930
Información de la política 1931
Versión de la política 1931
Documento de política JSON 1931
Más información 1936
AWSCompromisedKeyQuarantine 1936
Uso de la política 1936
Información de la política 1936
Versión de la política 1937
Documento de política JSON 1937
Más información 1938
AWSCompromisedKeyQuarantineV2 1938
Uso de la política 1938
Información de la política 1938
Versión de la política 1939
Documento de política JSON 1939
Más información 1941
AWSCompromisedKeyQuarantineV3 1941
Uso de la política 1942
Información de la política 1942
Versión de la política 1942
Documento de política JSON 1942
Más información 1945
AWSConfigMultiAccountSetupPolicy 1945
Uso de la política 1945
Información de la política 1945
Versión de la política 1945
Documento de política JSON 1946
Más información 1948

AWSConfigRemediationServiceRolePolicy 1948
Uso de la política 1948
Información de la política 1948
Versión de la política 1948
Documento de política JSON 1948
Más información 1949
AWSConfigRoleForOrganizations 1949
Uso de la política 1949
Información de la política 1949
Versión de la política 1950
Documento de política JSON 1950
Más información 1950
AWSConfigRulesExecutionRole 1951
Uso de la política 1951
Información de la política 1951
Versión de la política 1951
Documento de política JSON 1951
Más información 1952
AWSConfigServiceRolePolicy 1952
Uso de la política 1952
Información de la política 1952
Versión de la política 1953
Documento de política JSON 1953
Más información 1990
AWSConfigUserAccess 1991
Uso de la política 1991
Información de la política 1991
Versión de la política 1991
Documento de política JSON 1991
Más información 1992
AWSConnector 1992
Uso de la política 1992
Información de la política 1992
Versión de la política 1993
Documento de política JSON 1993
Más información 1995

AWSControlTowerAccountServiceRolePolicy 1995
Uso de la política 1995
Información de la política 1995
Versión de la política 1996
Documento de política JSON 1996
Más información 1998
AWSControlTowerServiceRolePolicy 1998
Uso de la política 1999
Información de la política 1999
Versión de la política 1999
Documento de política JSON 1999
Más información 2004
AWSCostAndUsageReportAutomationPolicy 2004
Uso de la política 2004
Información de la política 2004
Versión de la política 2005
Documento de política JSON 2005
Más información 2006
AWSDataExchangeDataGrantOwnerFullAccess 2006
Uso de la política 2006
Información de la política 2006
Versión de la política 2006
Documento de política JSON 2007
Más información 2008
AWSDataExchangeDataGrantReceiverFullAccess 2008
Uso de la política 2009
Información de la política 2009
Versión de la política 2009
Documento de política JSON 2009
Más información 2011
AWSDataExchangeFullAccess 2011
Uso de la política 2011
Información de la política 2011
Versión de la política 2011
Documento de política JSON 2012
Más información 2015

AWSDataExchangeProviderFullAccess 2015
Uso de la política 2015
Información de la política 2016
Versión de la política 2016
Documento de política JSON 2016
Más información 2020
AWSDataExchangeReadOnly 2020
Uso de la política 2020
Información de la política 2020
Versión de la política 2021
Documento de política JSON 2021
Más información 2022
AWSDataExchangeServiceRolePolicyForLicenseManagement 2022
Uso de la política 2022
Información de la política 2023
Versión de la política 2023
Documento de política JSON 2023
Más información 2024
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2024
Uso de la política 2024
Información de la política 2024
Versión de la política 2024
Documento de política JSON 2025
Más información 2025
AWSDataExchangeSubscriberFullAccess 2025
Uso de la política 2025
Información de la política 2026
Versión de la política 2026
Documento de política JSON 2026
Más información 2028
AWSDataLifecycleManagerServiceRole 2028
Uso de la política 2029
Información de la política 2029
Versión de la política 2029
Documento de política JSON 2029
Más información 2030

AWSDataLifecycleManagerServiceRoleForAMIManagement 2031
Uso de la política 2031
Información de la política 2031
Versión de la política 2031
Documento de política JSON 2031
Más información 2033
AWSDataLifecycleManagerSSMFullAccess 2033
Uso de la política 2033
Información de la política 2033
Versión de la política 2033
Documento de política JSON 2034
Más información 2035
AWSDataPipeline_FullAccess 2035
Uso de la política 2035
Información de la política 2035
Versión de la política 2036
Documento de política JSON 2036
Más información 2037
AWSDataPipeline_PowerUser 2037
Uso de la política 2037
Información de la política 2037
Versión de la política 2037
Documento de política JSON 2038
Más información 2039
AWSDataSyncDiscoveryServiceRolePolicy 2039
Uso de la política 2039
Información de la política 2039
Versión de la política 2039
Documento de política JSON 2040
Más información 2041
AWSDataSyncFullAccess 2041
Uso de la política 2041
Información de la política 2041
Versión de la política 2041
Documento de política JSON 2041
Más información 2044

AWSDataSyncReadOnlyAccess 2044
Uso de la política 2044
Información de la política 2044
Versión de la política 2045
Documento de política JSON 2045
Más información 2045
AWSDataSyncServiceRolePolicy 2046
Uso de la política 2046
Información de la política 2046
Versión de la política 2046
Documento de política JSON 2046
Más información 2047
AWSDeadlineCloud-FleetWorker 2048
Uso de la política 2048
Información de la política 2048
Versión de la política 2048
Documento de política JSON 2048
Más información 2049
AWSDeadlineCloud-UserAccessFarms 2049
Uso de la política 2049
Información de la política 2049
Versión de la política 2050
Documento de política JSON 2050
Más información 2055
AWSDeadlineCloud-UserAccessFleets 2055
Uso de la política 2056
Información de la política 2056
Versión de la política 2056
Documento de política JSON 2056
Más información 2060
AWSDeadlineCloud-UserAccessJobs 2060
Uso de la política 2060
Información de la política 2060
Versión de la política 2060
Documento de política JSON 2061
Más información 2065

AWSDeadlineCloud-UserAccessQueues 2065
Uso de la política 2065
Información de la política 2065
Versión de la política 2065
Documento de política JSON 2066
Más información 2070
AWSDeadlineCloud-WorkerHost 2070
Uso de la política 2071
Información de la política 2071
Versión de la política 2071
Documento de política JSON 2071
Más información 2072
AWSDeepLensLambdaFunctionAccessPolicy 2073
Uso de la política 2073
Información de la política 2073
Versión de la política 2073
Documento de política JSON 2073
Más información 2075
AWSDeepLensServiceRolePolicy 2075
Uso de la política 2075
Información de la política 2075
Versión de la política 2075
Documento de política JSON 2076
Más información 2083
AWSDeepRacerAccountAdminAccess 2083
Uso de la política 2083
Información de la política 2083
Versión de la política 2083
Documento de política JSON 2084
Más información 2084
AWSDeepRacerCloudFormationAccessPolicy 2084
Uso de la política 2085
Información de la política 2085
Versión de la política 2085
Documento de política JSON 2085
Más información 2088

AWSDeepRacerDefaultMultiUserAccess 2088
Uso de la política 2088
Información de la política 2088
Versión de la política 2089
Documento de política JSON 2089
Más información 2090
AWSDeepRacerFullAccess 2091
Uso de la política 2091
Información de la política 2091
Versión de la política 2091
Documento de política JSON 2091
Más información 2092
AWSDeepRacerRoboMakerAccessPolicy 2092
Uso de la política 2093
Información de la política 2093
Versión de la política 2093
Documento de política JSON 2093
Más información 2095
AWSDeepRacerServiceRolePolicy 2095
Uso de la política 2095
Información de la política 2096
Versión de la política 2096
Documento de política JSON 2096
Más información 2099
AWSDenyAll 2099
Uso de la política 2099
Información de la política 2100
Versión de la política 2100
Documento de política JSON 2100
Más información 2100
AWSDeviceFarmFullAccess 2101
Uso de la política 2101
Información de la política 2101
Versión de la política 2101
Documento de política JSON 2101
Más información 2102

AWSDeviceFarmServiceRolePolicy 2102
Uso de la política 2102
Información de la política 2102
Versión de la política 2102
Documento de política JSON 2103
Más información 2105
AWSDeviceFarmTestGridServiceRolePolicy 2105
Uso de la política 2105
Información de la política 2105
Versión de la política 2105
Documento de política JSON 2106
Más información 2108
AWSDirectConnectFullAccess 2108
Uso de la política 2108
Información de la política 2108
Versión de la política 2108
Documento de política JSON 2108
Más información 2109
AWSDirectConnectReadOnlyAccess 2109
Uso de la política 2109
Información de la política 2109
Versión de la política 2110
Documento de política JSON 2110
Más información 2110
AWSDirectConnectServiceRolePolicy 2111
Uso de la política 2111
Información de la política 2111
Versión de la política 2111
Documento de política JSON 2111
Más información 2112
AWSDirectoryServiceDataFullAccess 2112
Uso de la política 2112
Información de la política 2112
Versión de la política 2112
Documento de política JSON 2113
Más información 2113

AWSDirectoryServiceDataReadOnlyAccess 2114
Uso de la política 2114
Información de la política 2114
Versión de la política 2114
Documento de política JSON 2114
Más información 2115
AWSDirectoryServiceFullAccess 2115
Uso de la política 2115
Información de la política 2115
Versión de la política 2116
Documento de política JSON 2116
Más información 2118
AWSDirectoryServiceReadOnlyAccess 2118
Uso de la política 2118
Información de la política 2118
Versión de la política 2118
Documento de política JSON 2119
Más información 2119
AWSDiscoveryContinuousExportFirehosePolicy 2120
Uso de la política 2120
Información de la política 2120
Versión de la política 2120
Documento de política JSON 2120
Más información 2121
AWSDMSFleetAdvisorServiceRolePolicy 2121
Uso de la política 2122
Información de la política 2122
Versión de la política 2122
Documento de política JSON 2122
Más información 2123
AWSDMSServerlessServiceRolePolicy 2123
Uso de la política 2123
Información de la política 2123
Versión de la política 2123
Documento de política JSON 2123
Más información 2126

AWSEC2CapacityReservationFleetRolePolicy 2126
Uso de la política 2126
Información de la política 2127
Versión de la política 2127
Documento de política JSON 2127
Más información 2128
AWSEC2FleetServiceRolePolicy 2128
Uso de la política 2128
Información de la política 2129
Versión de la política 2129
Documento de política JSON 2129
Más información 2131
AWSEC2SpotFleetServiceRolePolicy 2131
Uso de la política 2131
Información de la política 2131
Versión de la política 2132
Documento de política JSON 2132
Más información 2134
AWSEC2SpotServiceRolePolicy 2134
Uso de la política 2134
Información de la política 2134
Versión de la política 2134
Documento de política JSON 2135
Más información 2136
AWSEC2VssSnapshotPolicy 2136
Uso de la política 2136
Información de la política 2136
Versión de la política 2137
Documento de política JSON 2137
Más información 2140
AWSECRPullThroughCache_ServiceRolePolicy 2140
Uso de la política 2141
Información de la política 2141
Versión de la política 2141
Documento de política JSON 2141
Más información 2142

AWSElasticBeanstalkCustomPlatformforEC2Role 2142
Uso de la política 2142
Información de la política 2143
Versión de la política 2143
Documento de política JSON 2143
Más información 2145
AWSElasticBeanstalkEnhancedHealth 2145
Uso de la política 2145
Información de la política 2145
Versión de la política 2145
Documento de política JSON 2146
Más información 2147
AWSElasticBeanstalkMaintenance 2147
Uso de la política 2147
Información de la política 2147
Versión de la política 2147
Documento de política JSON 2148
Más información 2148
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2149
Uso de la política 2149
Información de la política 2149
Versión de la política 2149
Documento de política JSON 2149
Más información 2156
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2157
Uso de la política 2157
Información de la política 2157
Versión de la política 2157
Documento de política JSON 2157
Más información 2163
AWSElasticBeanstalkMulticontainerDocker 2163
Uso de la política 2163
Información de la política 2163
Versión de la política 2163
Documento de política JSON 2164
Más información 2165

AWSElasticBeanstalkReadOnly 2165
Uso de la política 2165
Información de la política 2165
Versión de la política 2165
Documento de política JSON 2166
Más información 2168
AWSElasticBeanstalkRoleCore 2168
Uso de la política 2168
Información de la política 2168
Versión de la política 2168
Documento de política JSON 2169
Más información 2173
AWSElasticBeanstalkRoleCWL 2174
Uso de la política 2174
Información de la política 2174
Versión de la política 2174
Documento de política JSON 2174
Más información 2175
AWSElasticBeanstalkRoleECS 2175
Uso de la política 2175
Información de la política 2175
Versión de la política 2176
Documento de política JSON 2176
Más información 2177
AWSElasticBeanstalkRoleRDS 2177
Uso de la política 2177
Información de la política 2177
Versión de la política 2177
Documento de política JSON 2178
Más información 2178
AWSElasticBeanstalkRoleSNS 2178
Uso de la política 2179
Información de la política 2179
Versión de la política 2179
Documento de política JSON 2179
Más información 2180

AWSElasticBeanstalkRoleWorkerTier 2180
Uso de la política 2180
Información de la política 2180
Versión de la política 2181
Documento de política JSON 2181
Más información 2181
AWSElasticBeanstalkService 2182
Uso de la política 2182
Información de la política 2182
Versión de la política 2182
Documento de política JSON 2182
Más información 2187
AWSElasticBeanstalkServiceRolePolicy 2187
Uso de la política 2187
Información de la política 2187
Versión de la política 2187
Documento de política JSON 2188
Más información 2189
AWSElasticBeanstalkWebTier 2189
Uso de la política 2189
Información de la política 2189
Versión de la política 2190
Documento de política JSON 2190
Más información 2191
AWSElasticBeanstalkWorkerTier 2192
Uso de la política 2192
Información de la política 2192
Versión de la política 2192
Documento de política JSON 2192
Más información 2194
AWSElasticDisasterRecoveryAgentInstallationPolicy 2195
Uso de la política 2195
Información de la política 2195
Versión de la política 2195
Documento de política JSON 2195
Más información 2197

AWSElasticDisasterRecoveryAgentPolicy 2197
Uso de la política 2197
Información de la política 2197
Versión de la política 2198
Documento de política JSON 2198
Más información 2199
AWSElasticDisasterRecoveryConsoleFullAccess 2199
Uso de la política 2199
Información de la política 2199
Versión de la política 2199
Documento de política JSON 2200
Más información 2210
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2210
Uso de la política 2210
Información de la política 2210
Versión de la política 2211
Documento de política JSON 2211
Más información 2226
AWSElasticDisasterRecoveryConversionServerPolicy 2226
Uso de la política 2227
Información de la política 2227
Versión de la política 2227
Documento de política JSON 2227
Más información 2228
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2228
Uso de la política 2228
Información de la política 2229
Versión de la política 2229
Documento de política JSON 2229
Más información 2230
AWSElasticDisasterRecoveryEc2InstancePolicy 2230
Uso de la política 2230
Información de la política 2230
Versión de la política 2231
Documento de política JSON 2231
Más información 2233

AWSElasticDisasterRecoveryFailbackInstallationPolicy 2233
Uso de la política 2233
Información de la política 2233
Versión de la política 2234
Documento de política JSON 2234
Más información 2235
AWSElasticDisasterRecoveryFailbackPolicy 2235
Uso de la política 2235
Información de la política 2235
Versión de la política 2235
Documento de política JSON 2236
Más información 2237
AWSElasticDisasterRecoveryLaunchActionsPolicy 2237
Uso de la política 2237
Información de la política 2237
Versión de la política 2238
Documento de política JSON 2238
Más información 2244
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2244
Uso de la política 2244
Información de la política 2244
Versión de la política 2245
Documento de política JSON 2245
Más información 2246
AWSElasticDisasterRecoveryReadOnlyAccess 2246
Uso de la política 2246
Información de la política 2246
Versión de la política 2246
Documento de política JSON 2247
Más información 2249
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2249
Uso de la política 2249
Información de la política 2249
Versión de la política 2250
Documento de política JSON 2250
Más información 2252

AWSElasticDisasterRecoveryReplicationServerPolicy 2253
Uso de la política 2253
Información de la política 2253
Versión de la política 2253
Documento de política JSON 2254
Más información 2256
AWSElasticDisasterRecoveryServiceRolePolicy 2256
Uso de la política 2256
Información de la política 2256
Versión de la política 2256
Documento de política JSON 2257
Más información 2267
AWSElasticDisasterRecoveryStagingAccountPolicy 2267
Uso de la política 2267
Información de la política 2267
Versión de la política 2267
Documento de política JSON 2268
Más información 2268
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2269
Uso de la política 2269
Información de la política 2269
Versión de la política 2269
Documento de política JSON 2269
Más información 2271
AWSElasticLoadBalancingClassicServiceRolePolicy 2271
Uso de la política 2271
Información de la política 2271
Versión de la política 2271
Documento de política JSON 2272
Más información 2272
AWSElasticLoadBalancingServiceRolePolicy 2273
Uso de la política 2273
Información de la política 2273
Versión de la política 2273
Documento de política JSON 2273
Más información 2274

AWSElementalMediaConnectFullAccess 2275
Uso de la política 2275
Información de la política 2275
Versión de la política 2275
Documento de política JSON 2275
Más información 2276
AWSElementalMediaConnectReadOnlyAccess 2276
Uso de la política 2276
Información de la política 2276
Versión de la política 2276
Documento de política JSON 2276
Más información 2277
AWSElementalMediaConvertFullAccess 2277
Uso de la política 2278
Información de la política 2278
Versión de la política 2278
Documento de política JSON 2278
Más información 2279
AWSElementalMediaConvertReadOnly 2279
Uso de la política 2279
Información de la política 2279
Versión de la política 2280
Documento de política JSON 2280
Más información 2280
AWSElementalMediaLiveFullAccess 2280
Uso de la política 2281
Información de la política 2281
Versión de la política 2281
Documento de política JSON 2281
Más información 2281
AWSElementalMediaLiveReadOnly 2282
Uso de la política 2282
Información de la política 2282
Versión de la política 2282
Documento de política JSON 2282
Más información 2283

AWSElementalMediaPackageFullAccess 2283
Uso de la política 2283
Información de la política 2283
Versión de la política 2283
Documento de política JSON 2284
Más información 2284
AWSElementalMediaPackageReadOnly 2284
Uso de la política 2284
Información de la política 2284
Versión de la política 2285
Documento de política JSON 2285
Más información 2285
AWSElementalMediaPackageV2FullAccess 2285
Uso de la política 2286
Información de la política 2286
Versión de la política 2286
Documento de política JSON 2286
Más información 2286
AWSElementalMediaPackageV2ReadOnly 2287
Uso de la política 2287
Información de la política 2287
Versión de la política 2287
Documento de política JSON 2287
Más información 2288
AWSElementalMediaStoreFullAccess 2288
Uso de la política 2288
Información de la política 2288
Versión de la política 2288
Documento de política JSON 2289
Más información 2289
AWSElementalMediaStoreReadOnly 2289
Uso de la política 2290
Información de la política 2290
Versión de la política 2290
Documento de política JSON 2290
Más información 2291

AWSElementalMediaTailorFullAccess 2291
Uso de la política 2291
Información de la política 2291
Versión de la política 2291
Documento de política JSON 2291
Más información 2292
AWSElementalMediaTailorReadOnly 2292
Uso de la política 2292
Información de la política 2292
Versión de la política 2292
Documento de política JSON 2293
Más información 2293
AWSEnhancedClassicNetworkingMangementPolicy 2293
Uso de la política 2293
Información de la política 2294
Versión de la política 2294
Documento de política JSON 2294
Más información 2294
AWSEntityResolutionConsoleFullAccess 2295
Uso de la política 2295
Información de la política 2295
Versión de la política 2295
Documento de política JSON 2295
Más información 2298
AWSEntityResolutionConsoleReadOnlyAccess 2298
Uso de la política 2298
Información de la política 2298
Versión de la política 2299
Documento de política JSON 2299
Más información 2299
AWSFaultInjectionSimulatorEC2Access 2299
Uso de la política 2300
Información de la política 2300
Versión de la política 2300
Documento de política JSON 2300
Más información 2302

AWSFaultInjectionSimulatorECSAccess 2302
Uso de la política 2302
Información de la política 2302
Versión de la política 2302
Documento de política JSON 2303
Más información 2304
AWSFaultInjectionSimulatorEKSAccess 2305
Uso de la política 2305
Información de la política 2305
Versión de la política 2305
Documento de política JSON 2305
Más información 2306
AWSFaultInjectionSimulatorNetworkAccess 2307
Uso de la política 2307
Información de la política 2307
Versión de la política 2307
Documento de política JSON 2307
Más información 2314
AWSFaultInjectionSimulatorRDSAccess 2315
Uso de la política 2315
Información de la política 2315
Versión de la política 2315
Documento de política JSON 2315
Más información 2316
AWSFaultInjectionSimulatorSSMAccess 2317
Uso de la política 2317
Información de la política 2317
Versión de la política 2317
Documento de política JSON 2317
Más información 2319
AWSFinSpaceServiceRolePolicy 2319
Uso de la política 2319
Información de la política 2319
Versión de la política 2319
Documento de política JSON 2320
Más información 2320

AWSFMAdminFullAccess 2320
Uso de la política 2320
Información de la política 2321
Versión de la política 2321
Documento de política JSON 2321
Más información 2323
AWSFMAdminReadOnlyAccess 2323
Uso de la política 2323
Información de la política 2323
Versión de la política 2324
Documento de política JSON 2324
Más información 2325
AWSFMMemberReadOnlyAccess 2326
Uso de la política 2326
Información de la política 2326
Versión de la política 2326
Documento de política JSON 2326
Más información 2327
AWSForWordPressPluginPolicy 2327
Uso de la política 2327
Información de la política 2327
Versión de la política 2327
Documento de política JSON 2328
Más información 2329
AWSGitSyncServiceRolePolicy 2330
Uso de la política 2330
Información de la política 2330
Versión de la política 2330
Documento de política JSON 2330
Más información 2331
AWSGlobalAcceleratorSLRPolicy 2331
Uso de la política 2331
Información de la política 2331
Versión de la política 2332
Documento de política JSON 2332
Más información 2333

AWSGlueConsoleFullAccess 2334
Uso de la política 2334
Información de la política 2334
Versión de la política 2334
Documento de política JSON 2334
Más información 2338
AWSGlueConsoleSageMakerNotebookFullAccess 2339
Uso de la política 2339
Información de la política 2339
Versión de la política 2339
Documento de política JSON 2339
Más información 2345
AwsGlueDataBrewFullAccessPolicy 2345
Uso de la política 2345
Información de la política 2345
Versión de la política 2345
Documento de política JSON 2346
Más información 2351
AWSGlueDataBrewServiceRole 2351
Uso de la política 2351
Información de la política 2351
Versión de la política 2351
Documento de política JSON 2352
Más información 2354
AWSGlueSchemaRegistryFullAccess 2355
Uso de la política 2355
Información de la política 2355
Versión de la política 2355
Documento de política JSON 2355
Más información 2357
AWSGlueSchemaRegistryReadonlyAccess 2357
Uso de la política 2357
Información de la política 2357
Versión de la política 2357
Documento de política JSON 2357
Más información 2358

AWSGlueServiceNotebookRole 2358
Uso de la política 2359
Información de la política 2359
Versión de la política 2359
Documento de política JSON 2359
Más información 2361
AWSGlueServiceRole 2362
Uso de la política 2362
Información de la política 2362
Versión de la política 2362
Documento de política JSON 2362
Más información 2365
AwsGlueSessionUserRestrictedNotebookPolicy 2365
Uso de la política 2365
Información de la política 2365
Versión de la política 2365
Documento de política JSON 2366
Más información 2368
AwsGlueSessionUserRestrictedNotebookServiceRole 2369
Uso de la política 2369
Información de la política 2369
Versión de la política 2369
Documento de política JSON 2369
Más información 2373
AwsGlueSessionUserRestrictedPolicy 2374
Uso de la política 2374
Información de la política 2374
Versión de la política 2374
Documento de política JSON 2374
Más información 2377
AwsGlueSessionUserRestrictedServiceRole 2377
Uso de la política 2377
Información de la política 2378
Versión de la política 2378
Documento de política JSON 2378
Más información 2382

AWSGrafanaAccountAdministrator 2383
Uso de la política 2383
Información de la política 2383
Versión de la política 2383
Documento de política JSON 2383
Más información 2384
AWSGrafanaConsoleReadOnlyAccess 2384
Uso de la política 2385
Información de la política 2385
Versión de la política 2385
Documento de política JSON 2385
Más información 2386
AWSGrafanaWorkspacePermissionManagement 2386
Uso de la política 2386
Información de la política 2386
Versión de la política 2386
Documento de política JSON 2387
Más información 2387
AWSGrafanaWorkspacePermissionManagementV2 2388
Uso de la política 2388
Información de la política 2388
Versión de la política 2388
Documento de política JSON 2388
Más información 2389
AWSGreengrassFullAccess 2390
Uso de la política 2390
Información de la política 2390
Versión de la política 2390
Documento de política JSON 2390
Más información 2391
AWSGreengrassReadOnlyAccess 2391
Uso de la política 2391
Información de la política 2391
Versión de la política 2391
Documento de política JSON 2392
Más información 2392

AWSGreengrassResourceAccessRolePolicy 2392
Uso de la política 2392
Información de la política 2392
Versión de la política 2393
Documento de política JSON 2393
Más información 2395
AWSGroundStationAgentInstancePolicy 2395
Uso de la política 2396
Información de la política 2396
Versión de la política 2396
Documento de política JSON 2396
Más información 2397
AWSHealth_EventProcessorServiceRolePolicy 2397
Uso de la política 2397
Información de la política 2397
Versión de la política 2397
Documento de política JSON 2398
Más información 2398
AWSHealthFullAccess 2399
Uso de la política 2399
Información de la política 2399
Versión de la política 2399
Documento de política JSON 2399
Más información 2400
AWSHealthImagingFullAccess 2400
Uso de la política 2401
Información de la política 2401
Versión de la política 2401
Documento de política JSON 2401
Más información 2402
AWSHealthImagingReadOnlyAccess 2402
Uso de la política 2402
Información de la política 2402
Versión de la política 2402
Documento de política JSON 2403
Más información 2403

AWSIAMIdentityCenterAllowListForIdentityContext 2404
Uso de la política 2404
Información de la política 2404
Versión de la política 2404
Documento de política JSON 2404
Más información 2407
AWSIdentitySyncFullAccess 2408
Uso de la política 2408
Información de la política 2408
Versión de la política 2408
Documento de política JSON 2408
Más información 2409
AWSIdentitySyncReadOnlyAccess 2409
Uso de la política 2410
Información de la política 2410
Versión de la política 2410
Documento de política JSON 2410
Más información 2411
AWSImageBuilderFullAccess 2411
Uso de la política 2411
Información de la política 2411
Versión de la política 2411
Documento de política JSON 2412
Más información 2414
AWSImageBuilderReadOnlyAccess 2414
Uso de la política 2415
Información de la política 2415
Versión de la política 2415
Documento de política JSON 2415
Más información 2416
AWSImportExportFullAccess 2416
Uso de la política 2416
Información de la política 2416
Versión de la política 2416
Documento de política JSON 2417
Más información 2417

AWSImportExportReadOnlyAccess 2417
Uso de la política 2417
Información de la política 2418
Versión de la política 2418
Documento de política JSON 2418
Más información 2418
AWSIncidentManagerIncidentAccessServiceRolePolicy 2419
Uso de la política 2419
Información de la política 2419
Versión de la política 2419
Documento de política JSON 2419
Más información 2420
AWSIncidentManagerResolverAccess 2420
Uso de la política 2420
Información de la política 2420
Versión de la política 2421
Documento de política JSON 2421
Más información 2422
AWSIncidentManagerServiceRolePolicy 2422
Uso de la política 2422
Información de la política 2422
Versión de la política 2423
Documento de política JSON 2423
Más información 2424
AWSIoT1ClickFullAccess 2424
Uso de la política 2424
Información de la política 2424
Versión de la política 2425
Documento de política JSON 2425
Más información 2425
AWSIoT1ClickReadOnlyAccess 2425
Uso de la política 2426
Información de la política 2426
Versión de la política 2426
Documento de política JSON 2426
Más información 2427

AWSIoTAnalyticsFullAccess 2427
Uso de la política 2427
Información de la política 2427
Versión de la política 2427
Documento de política JSON 2427
Más información 2428
AWSIoTAnalyticsReadOnlyAccess 2428
Uso de la política 2428
Información de la política 2428
Versión de la política 2429
Documento de política JSON 2429
Más información 2429
AWSIoTConfigAccess 2429
Uso de la política 2430
Información de la política 2430
Versión de la política 2430
Documento de política JSON 2430
Más información 2434
AWSIoTConfigReadOnlyAccess 2434
Uso de la política 2434
Información de la política 2434
Versión de la política 2435
Documento de política JSON 2435
Más información 2437
AWSIoTDataAccess 2437
Uso de la política 2437
Información de la política 2437
Versión de la política 2437
Documento de política JSON 2438
Más información 2438
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2439
Uso de la política 2439
Información de la política 2439
Versión de la política 2439
Documento de política JSON 2439
Más información 2440

AWSIoTDeviceDefenderAudit 2440
Uso de la política 2440
Información de la política 2440
Versión de la política 2440
Documento de política JSON 2441
Más información 2442
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2442
Uso de la política 2442
Información de la política 2442
Versión de la política 2442
Documento de política JSON 2443
Más información 2443
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2444
Uso de la política 2444
Información de la política 2444
Versión de la política 2444
Documento de política JSON 2444
Más información 2445
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2445
Uso de la política 2445
Información de la política 2445
Versión de la política 2446
Documento de política JSON 2446
Más información 2446
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2446
Uso de la política 2447
Información de la política 2447
Versión de la política 2447
Documento de política JSON 2447
Más información 2448
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2448
Uso de la política 2448
Información de la política 2448
Versión de la política 2448
Documento de política JSON 2449
Más información 2449

AWSIoTDeviceTesterForFreeRTOSFullAccess 2449
Uso de la política 2450
Información de la política 2450
Versión de la política 2450
Documento de política JSON 2450
Más información 2456
AWSIoTDeviceTesterForGreengrassFullAccess 2456
Uso de la política 2457
Información de la política 2457
Versión de la política 2457
Documento de política JSON 2457
Más información 2460
AWSIoTEventsFullAccess 2460
Uso de la política 2460
Información de la política 2460
Versión de la política 2461
Documento de política JSON 2461
Más información 2461
AWSIoTEventsReadOnlyAccess 2462
Uso de la política 2462
Información de la política 2462
Versión de la política 2462
Documento de política JSON 2462
Más información 2463
AWSIoTFleetHubFederationAccess 2463
Uso de la política 2463
Información de la política 2463
Versión de la política 2463
Documento de política JSON 2464
Más información 2465
AWSIoTFleetwiseServiceRolePolicy 2466
Uso de la política 2466
Información de la política 2466
Versión de la política 2466
Documento de política JSON 2466
Más información 2467

AWSIoTFullAccess 2467
Uso de la política 2467
Información de la política 2467
Versión de la política 2467
Documento de política JSON 2468
Más información 2468
AWSIoTLogging 2468
Uso de la política 2468
Información de la política 2469
Versión de la política 2469
Documento de política JSON 2469
Más información 2470
AWSIoTManagedIntegrationsFullAccess 2470
Uso de la política 2470
Información de la política 2470
Versión de la política 2470
Documento de política JSON 2471
Más información 2471
AWSIoTManagedIntegrationsRolePolicy 2471
Uso de la política 2472
Información de la política 2472
Versión de la política 2472
Documento de política JSON 2472
Más información 2473
AWSIoTOTAUpdate 2474
Uso de la política 2474
Información de la política 2474
Versión de la política 2474
Documento de política JSON 2474
Más información 2475
AWSIotRoboRunnerFullAccess 2475
Uso de la política 2475
Información de la política 2475
Versión de la política 2475
Documento de política JSON 2476
Más información 2476

AWSIotRoboRunnerReadOnly 2476
Uso de la política 2477
Información de la política 2477
Versión de la política 2477
Documento de política JSON 2477
Más información 2478
AWSIotRoboRunnerServiceRolePolicy 2478
Uso de la política 2478
Información de la política 2478
Versión de la política 2478
Documento de política JSON 2479
Más información 2479
AWSIoTRuleActions 2479
Uso de la política 2479
Información de la política 2479
Versión de la política 2480
Documento de política JSON 2480
Más información 2480
AWSIoTSiteWiseConsoleFullAccess 2481
Uso de la política 2481
Información de la política 2481
Versión de la política 2481
Documento de política JSON 2481
Más información 2484
AWSIoTSiteWiseFullAccess 2484
Uso de la política 2484
Información de la política 2484
Versión de la política 2484
Documento de política JSON 2484
Más información 2485
AWSIoTSiteWiseMonitorPortalAccess 2485
Uso de la política 2485
Información de la política 2485
Versión de la política 2486
Documento de política JSON 2486
Más información 2487

AWSIoTSiteWiseMonitorServiceRolePolicy 2487
Uso de la política 2487
Información de la política 2487
Versión de la política 2488
Documento de política JSON 2488
Más información 2489
AWSIoTSiteWiseReadOnlyAccess 2489
Uso de la política 2489
Información de la política 2489
Versión de la política 2489
Documento de política JSON 2490
Más información 2490
AWSIoTThingsRegistration 2490
Uso de la política 2490
Información de la política 2491
Versión de la política 2491
Documento de política JSON 2491
Más información 2492
AWSIoTTwinMakerServiceRolePolicy 2492
Uso de la política 2493
Información de la política 2493
Versión de la política 2493
Documento de política JSON 2493
Más información 2495
AWSIoTWirelessDataAccess 2495
Uso de la política 2495
Información de la política 2495
Versión de la política 2495
Documento de política JSON 2495
Más información 2496
AWSIoTWirelessFullAccess 2496
Uso de la política 2496
Información de la política 2496
Versión de la política 2497
Documento de política JSON 2497
Más información 2497

AWSIoTWirelessFullPublishAccess 2497
Uso de la política 2498
Información de la política 2498
Versión de la política 2498
Documento de política JSON 2498
Más información 2498
AWSIoTWirelessGatewayCertManager 2499
Uso de la política 2499
Información de la política 2499
Versión de la política 2499
Documento de política JSON 2499
Más información 2500
AWSIoTWirelessLogging 2500
Uso de la política 2500
Información de la política 2500
Versión de la política 2501
Documento de política JSON 2501
Más información 2501
AWSIoTWirelessReadOnlyAccess 2502
Uso de la política 2502
Información de la política 2502
Versión de la política 2502
Documento de política JSON 2502
Más información 2503
AWSIPAMServiceRolePolicy 2503
Uso de la política 2503
Información de la política 2503
Versión de la política 2503
Documento de política JSON 2504
Más información 2505
AWSIQContractServiceRolePolicy 2505
Uso de la política 2505
Información de la política 2505
Versión de la política 2505
Documento de política JSON 2506
Más información 2506

AWSIQFullAccess 2506
Uso de la política 2506
Información de la política 2506
Versión de la política 2507
Documento de política JSON 2507
Más información 2508
AWSIQPermissionServiceRolePolicy 2508
Uso de la política 2508
Información de la política 2508
Versión de la política 2508
Documento de política JSON 2509
Más información 2509
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2510
Uso de la política 2510
Información de la política 2510
Versión de la política 2510
Documento de política JSON 2510
Más información 2511
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2511
Uso de la política 2511
Información de la política 2511
Versión de la política 2512
Documento de política JSON 2512
Más información 2512
AWSKeyManagementServicePowerUser 2512
Uso de la política 2513
Información de la política 2513
Versión de la política 2513
Documento de política JSON 2513
Más información 2514
AWSLakeFormationCrossAccountManager 2514
Uso de la política 2514
Información de la política 2514
Versión de la política 2514
Documento de política JSON 2515
Más información 2517

AWSLakeFormationDataAdmin 2517
Uso de la política 2517
Información de la política 2517
Versión de la política 2517
Documento de política JSON 2518
Más información 2519
AWSLambda_FullAccess 2519
Uso de la política 2519
Información de la política 2519
Versión de la política 2520
Documento de política JSON 2520
Más información 2521
AWSLambda_ReadOnlyAccess 2522
Uso de la política 2522
Información de la política 2522
Versión de la política 2522
Documento de política JSON 2522
Más información 2524
AWSLambdaBasicExecutionRole 2524
Uso de la política 2524
Información de la política 2524
Versión de la política 2524
Documento de política JSON 2524
Más información 2525
AWSLambdaDynamoDBExecutionRole 2525
Uso de la política 2525
Información de la política 2525
Versión de la política 2526
Documento de política JSON 2526
Más información 2526
AWSLambdaENIManagementAccess 2527
Uso de la política 2527
Información de la política 2527
Versión de la política 2527
Documento de política JSON 2527
Más información 2528

AWSLambdaExecute 2528
Uso de la política 2528
Información de la política 2528
Versión de la política 2528
Documento de política JSON 2529
Más información 2529
AWSLambdaFullAccess 2530
Uso de la política 2530
Información de la política 2530
Versión de la política 2530
Documento de política JSON 2530
Más información 2532
AWSLambdaInvocation-DynamoDB 2532
Uso de la política 2532
Información de la política 2532
Versión de la política 2533
Documento de política JSON 2533
Más información 2533
AWSLambdaKinesisExecutionRole 2534
Uso de la política 2534
Información de la política 2534
Versión de la política 2534
Documento de política JSON 2534
Más información 2535
AWSLambdaMSKExecutionRole 2535
Uso de la política 2535
Información de la política 2535
Versión de la política 2536
Documento de política JSON 2536
Más información 2536
AWSLambdaReplicator 2537
Uso de la política 2537
Información de la política 2537
Versión de la política 2537
Documento de política JSON 2537
Más información 2538

AWSLambdaRole 2539
Uso de la política 2539
Información de la política 2539
Versión de la política 2539
Documento de política JSON 2539
Más información 2540
AWSLambdaSQSQueueExecutionRole 2540
Uso de la política 2540
Información de la política 2540
Versión de la política 2540
Documento de política JSON 2541
Más información 2541
AWSLambdaVPCAccessExecutionRole 2541
Uso de la política 2542
Información de la política 2542
Versión de la política 2542
Documento de política JSON 2542
Más información 2543
AWSLicenseManagerConsumptionPolicy 2543
Uso de la política 2543
Información de la política 2543
Versión de la política 2543
Documento de política JSON 2544
Más información 2544
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2544
Uso de la política 2545
Información de la política 2545
Versión de la política 2545
Documento de política JSON 2545
Más información 2547
AWSLicenseManagerMasterAccountRolePolicy 2547
Uso de la política 2547
Información de la política 2547
Versión de la política 2548
Documento de política JSON 2548
Más información 2553

AWSLicenseManagerMemberAccountRolePolicy 2553
Uso de la política 2553
Información de la política 2553
Versión de la política 2553
Documento de política JSON 2553
Más información 2555
AWSLicenseManagerServiceRolePolicy 2555
Uso de la política 2555
Información de la política 2555
Versión de la política 2555
Documento de política JSON 2555
Más información 2559
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2559
Uso de la política 2559
Información de la política 2559
Versión de la política 2559
Documento de política JSON 2560
Más información 2562
AWSM2ServicePolicy 2563
Uso de la política 2563
Información de la política 2563
Versión de la política 2563
Documento de política JSON 2563
Más información 2565
AWSManagedServices_ContactsServiceRolePolicy 2565
Uso de la política 2565
Información de la política 2565
Versión de la política 2565
Documento de política JSON 2566
Más información 2566
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2567
Uso de la política 2567
Información de la política 2567
Versión de la política 2567
Documento de política JSON 2567
Más información 2569

AWSManagedServices_EventsServiceRolePolicy 2569
Uso de la política 2569
Información de la política 2569
Versión de la política 2569
Documento de política JSON 2570
Más información 2570
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2571
Uso de la política 2571
Información de la política 2571
Versión de la política 2571
Documento de política JSON 2571
Más información 2572
AWSManagedServicesDeploymentToolkitPolicy 2572
Uso de la política 2572
Información de la política 2572
Versión de la política 2573
Documento de política JSON 2573
Más información 2575
AWSMarketplaceAmiIngestion 2575
Uso de la política 2575
Información de la política 2575
Versión de la política 2576
Documento de política JSON 2576
Más información 2576
AWSMarketplaceDeploymentServiceRolePolicy 2577
Uso de la política 2577
Información de la política 2577
Versión de la política 2577
Documento de política JSON 2577
Más información 2579
AWSMarketplaceFullAccess 2579
Uso de la política 2579
Información de la política 2579
Versión de la política 2579
Documento de política JSON 2580
Más información 2581

AWSMarketplaceGetEntitlements 2582
Uso de la política 2582
Información de la política 2582
Versión de la política 2582
Documento de política JSON 2582
Más información 2583
AWSMarketplaceImageBuildFullAccess 2583
Uso de la política 2583
Información de la política 2583
Versión de la política 2583
Documento de política JSON 2584
Más información 2587
AWSMarketplaceLicenseManagementServiceRolePolicy 2587
Uso de la política 2588
Información de la política 2588
Versión de la política 2588
Documento de política JSON 2588
Más información 2589
AWSMarketplaceManageSubscriptions 2589
Uso de la política 2589
Información de la política 2589
Versión de la política 2589
Documento de política JSON 2590
Más información 2591
AWSMarketplaceMeteringFullAccess 2591
Uso de la política 2591
Información de la política 2591
Versión de la política 2592
Documento de política JSON 2592
Más información 2592
AWSMarketplaceMeteringRegisterUsage 2592
Uso de la política 2593
Información de la política 2593
Versión de la política 2593
Documento de política JSON 2593
Más información 2593

AWSMarketplaceProcurementSystemAdminFullAccess 2594
Uso de la política 2594
Información de la política 2594
Versión de la política 2594
Documento de política JSON 2594
Más información 2595
AWSMarketplacePurchaseOrdersServiceRolePolicy 2595
Uso de la política 2595
Información de la política 2595
Versión de la política 2596
Documento de política JSON 2596
Más información 2596
AWSMarketplaceRead-only 2596
Uso de la política 2597
Información de la política 2597
Versión de la política 2597
Documento de política JSON 2597
Más información 2598
AWSMarketplaceResaleAuthorizationServiceRolePolicy 2599
Uso de la política 2599
Información de la política 2599
Versión de la política 2599
Documento de política JSON 2599
Más información 2602
AWSMarketplaceSellerFullAccess 2602
Uso de la política 2602
Información de la política 2602
Versión de la política 2602
Documento de política JSON 2602
Más información 2606
AWSMarketplaceSellerOfferManagement 2606
Uso de la política 2606
Información de la política 2606
Versión de la política 2607
Documento de política JSON 2607
Más información 2609

AWSMarketplaceSellerProductsFullAccess 2609
Uso de la política 2609
Información de la política 2609
Versión de la política 2609
Documento de política JSON 2610
Más información 2611
AWSMarketplaceSellerProductsReadOnly 2612
Uso de la política 2612
Información de la política 2612
Versión de la política 2612
Documento de política JSON 2612
Más información 2613
AWSMediaConnectServicePolicy 2613
Uso de la política 2614
Información de la política 2614
Versión de la política 2614
Documento de política JSON 2614
Más información 2615
AWSMediaLiveAnywhereServiceRolePolicy 2616
Uso de la política 2616
Información de la política 2616
Versión de la política 2616
Documento de política JSON 2616
Más información 2619
AWSMediaTailorServiceRolePolicy 2619
Uso de la política 2619
Información de la política 2620
Versión de la política 2620
Documento de política JSON 2620
Más información 2621
AWSMigrationHubDiscoveryAccess 2621
Uso de la política 2621
Información de la política 2621
Versión de la política 2621
Documento de política JSON 2621
Más información 2623

AWSMigrationHubDMSAccess 2623
Uso de la política 2623
Información de la política 2623
Versión de la política 2623
Documento de política JSON 2624
Más información 2625
AWSMigrationHubFullAccess 2625
Uso de la política 2625
Información de la política 2625
Versión de la política 2625
Documento de política JSON 2625
Más información 2627
AWSMigrationHubOrchestratorConsoleFullAccess 2627
Uso de la política 2627
Información de la política 2627
Versión de la política 2628
Documento de política JSON 2628
Más información 2631
AWSMigrationHubOrchestratorInstanceRolePolicy 2631
Uso de la política 2631
Información de la política 2631
Versión de la política 2632
Documento de política JSON 2632
Más información 2633
AWSMigrationHubOrchestratorPlugin 2633
Uso de la política 2633
Información de la política 2633
Versión de la política 2633
Documento de política JSON 2634
Más información 2635
AWSMigrationHubOrchestratorServiceRolePolicy 2635
Uso de la política 2635
Información de la política 2635
Versión de la política 2636
Documento de política JSON 2636
Más información 2639

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2639
Uso de la política 2640
Información de la política 2640
Versión de la política 2640
Documento de política JSON 2640
Más información 2646
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2646
Uso de la política 2646
Información de la política 2646
Versión de la política 2647
Documento de política JSON 2647
Más información 2648
AWSMigrationHubRefactorSpacesFullAccess 2649
Uso de la política 2649
Información de la política 2649
Versión de la política 2649
Documento de política JSON 2649
Más información 2656
AWSMigrationHubRefactorSpacesServiceRolePolicy 2656
Uso de la política 2656
Información de la política 2656
Versión de la política 2657
Documento de política JSON 2657
Más información 2660
AWSMigrationHubSMSAccess 2661
Uso de la política 2661
Información de la política 2661
Versión de la política 2661
Documento de política JSON 2661
Más información 2662
AWSMigrationHubStrategyCollector 2662
Uso de la política 2663
Información de la política 2663
Versión de la política 2663
Documento de política JSON 2663
Más información 2665

AWSMigrationHubStrategyConsoleFullAccess 2666
Uso de la política 2666
Información de la política 2666
Versión de la política 2666
Documento de política JSON 2666
Más información 2668
AWSMigrationHubStrategyServiceRolePolicy 2668
Uso de la política 2668
Información de la política 2669
Versión de la política 2669
Documento de política JSON 2669
Más información 2670
AWSMobileHub_FullAccess 2670
Uso de la política 2670
Información de la política 2670
Versión de la política 2671
Documento de política JSON 2671
Más información 2672
AWSMobileHub_ReadOnly 2672
Uso de la política 2673
Información de la política 2673
Versión de la política 2673
Documento de política JSON 2673
Más información 2674
AWSMSKReplicatorExecutionRole 2675
Uso de la política 2675
Información de la política 2675
Versión de la política 2675
Documento de política JSON 2675
Más información 2677
AWSNetworkFirewallFullAccess 2677
Uso de la política 2677
Información de la política 2677
Versión de la política 2677
Documento de política JSON 2678
Más información 2681

AWSNetworkFirewallReadOnlyAccess 2682
Uso de la política 2682
Información de la política 2682
Versión de la política 2682
Documento de política JSON 2682
Más información 2683
AWSNetworkFirewallServiceRolePolicy 2684
Uso de la política 2684
Información de la política 2684
Versión de la política 2684
Documento de política JSON 2684
Más información 2686
AWSNetworkManagerCloudWANServiceRolePolicy 2686
Uso de la política 2686
Información de la política 2686
Versión de la política 2686
Documento de política JSON 2687
Más información 2687
AWSNetworkManagerFullAccess 2687
Uso de la política 2687
Información de la política 2688
Versión de la política 2688
Documento de política JSON 2688
Más información 2689
AWSNetworkManagerReadOnlyAccess 2689
Uso de la política 2689
Información de la política 2689
Versión de la política 2689
Documento de política JSON 2690
Más información 2690
AWSNetworkManagerServiceRolePolicy 2690
Uso de la política 2690
Información de la política 2691
Versión de la política 2691
Documento de política JSON 2691
Más información 2692

AWSObservabilityAdminServiceRolePolicy 2692
Uso de la política 2692
Información de la política 2692
Versión de la política 2693
Documento de política JSON 2693
Más información 2695
AWSOpsWorks_FullAccess 2696
Uso de la política 2696
Información de la política 2696
Versión de la política 2696
Documento de política JSON 2696
Más información 2697
AWSOpsWorksCloudWatchLogs 2698
Uso de la política 2698
Información de la política 2698
Versión de la política 2698
Documento de política JSON 2698
Más información 2699
AWSOpsWorksCMInstanceProfileRole 2699
Uso de la política 2699
Información de la política 2699
Versión de la política 2699
Documento de política JSON 2700
Más información 2701
AWSOpsWorksCMServiceRole 2701
Uso de la política 2701
Información de la política 2701
Versión de la política 2701
Documento de política JSON 2702
Más información 2706
AWSOpsWorksInstanceRegistration 2706
Uso de la política 2706
Información de la política 2706
Versión de la política 2706
Documento de política JSON 2707
Más información 2707

AWSOpsWorksRegisterCLI_EC2 2707
Uso de la política 2708
Información de la política 2708
Versión de la política 2708
Documento de política JSON 2708
Más información 2709
AWSOpsWorksRegisterCLI_OnPremises 2709
Uso de la política 2709
Información de la política 2709
Versión de la política 2710
Documento de política JSON 2710
Más información 2711
AWSOrganizationsFullAccess 2712
Uso de la política 2712
Información de la política 2712
Versión de la política 2712
Documento de política JSON 2712
Más información 2713
AWSOrganizationsReadOnlyAccess 2713
Uso de la política 2714
Información de la política 2714
Versión de la política 2714
Documento de política JSON 2714
Más información 2715
AWSOrganizationsServiceTrustPolicy 2715
Uso de la política 2715
Información de la política 2715
Versión de la política 2716
Documento de política JSON 2716
Más información 2716
AWSOutpostsAuthorizeServerPolicy 2717
Uso de la política 2717
Información de la política 2717
Versión de la política 2717
Documento de política JSON 2717
Más información 2718

AWSOutpostsServiceRolePolicy 2718
Uso de la política 2718
Información de la política 2718
Versión de la política 2719
Documento de política JSON 2719
Más información 2720
AWSPanoramaApplianceRolePolicy 2721
Uso de la política 2721
Información de la política 2721
Versión de la política 2721
Documento de política JSON 2721
Más información 2722
AWSPanoramaApplianceServiceRolePolicy 2722
Uso de la política 2722
Información de la política 2722
Versión de la política 2723
Documento de política JSON 2723
Más información 2724
AWSPanoramaFullAccess 2725
Uso de la política 2725
Información de la política 2725
Versión de la política 2725
Documento de política JSON 2725
Más información 2728
AWSPanoramaGreengrassGroupRolePolicy 2728
Uso de la política 2728
Información de la política 2728
Versión de la política 2728
Documento de política JSON 2729
Más información 2730
AWSPanoramaSageMakerRolePolicy 2730
Uso de la política 2730
Información de la política 2730
Versión de la política 2731
Documento de política JSON 2731
Más información 2731

AWSPanoramaServiceLinkedRolePolicy 2732
Uso de la política 2732
Información de la política 2732
Versión de la política 2732
Documento de política JSON 2732
Más información 2735
AWSPanoramaServiceRolePolicy 2735
Uso de la política 2735
Información de la política 2735
Versión de la política 2736
Documento de política JSON 2736
Más información 2743
AWSPartnerCentralFullAccess 2743
Uso de la política 2743
Información de la política 2743
Versión de la política 2743
Documento de política JSON 2744
Más información 2745
AWSPartnerCentralOpportunityManagement 2745
Uso de la política 2745
Información de la política 2746
Versión de la política 2746
Documento de política JSON 2746
Más información 2748
AWSPartnerCentralSandboxFullAccess 2748
Uso de la política 2748
Información de la política 2748
Versión de la política 2748
Documento de política JSON 2749
Más información 2749
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 2750
Uso de la política 2750
Información de la política 2750
Versión de la política 2750
Documento de política JSON 2750
Más información 2751

AWSPartnerLedSupportReadOnlyAccess 2751
Uso de la política 2752
Información de la política 2752
Versión de la política 2752
Documento de política JSON 2752
Más información 2789
AWSPCSComputeNodePolicy 2789
Uso de la política 2789
Información de la política 2789
Versión de la política 2790
Documento de política JSON 2790
Más información 2790
AWSPCSServiceRolePolicy 2791
Uso de la política 2791
Información de la política 2791
Versión de la política 2791
Documento de política JSON 2791
Más información 2796
AWSPriceListServiceFullAccess 2796
Uso de la política 2796
Información de la política 2797
Versión de la política 2797
Documento de política JSON 2797
Más información 2797
AWSPrivateCAAuditor 2798
Uso de la política 2798
Información de la política 2798
Versión de la política 2798
Documento de política JSON 2798
Más información 2799
AWSPrivateCAConnectorForKubernetesPolicy 2799
Uso de la política 2799
Información de la política 2800
Versión de la política 2800
Documento de política JSON 2800
Más información 2800

AWSPrivateCAFullAccess 2801
Uso de la política 2801
Información de la política 2801
Versión de la política 2801
Documento de política JSON 2801
Más información 2802
AWSPrivateCAPrivilegedUser 2802
Uso de la política 2802
Información de la política 2802
Versión de la política 2802
Documento de política JSON 2803
Más información 2804
AWSPrivateCAReadOnly 2804
Uso de la política 2804
Información de la política 2804
Versión de la política 2805
Documento de política JSON 2805
Más información 2805
AWSPrivateCAUser 2806
Uso de la política 2806
Información de la política 2806
Versión de la política 2806
Documento de política JSON 2806
Más información 2807
AWSPrivateMarketplaceAdminFullAccess 2808
Uso de la política 2808
Información de la política 2808
Versión de la política 2808
Documento de política JSON 2808
Más información 2811
AWSPrivateMarketplaceRequests 2811
Uso de la política 2811
Información de la política 2812
Versión de la política 2812
Documento de política JSON 2812
Más información 2812

AWSPrivateNetworksServiceRolePolicy 2813
Uso de la política 2813
Información de la política 2813
Versión de la política 2813
Documento de política JSON 2813
Más información 2814
AWSProtonCodeBuildProvisioningBasicAccess 2814
Uso de la política 2814
Información de la política 2814
Versión de la política 2815
Documento de política JSON 2815
Más información 2815
AWSProtonCodeBuildProvisioningServiceRolePolicy 2816
Uso de la política 2816
Información de la política 2816
Versión de la política 2816
Documento de política JSON 2816
Más información 2818
AWSProtonDeveloperAccess 2818
Uso de la política 2818
Información de la política 2818
Versión de la política 2818
Documento de política JSON 2818
Más información 2821
AWSProtonFullAccess 2821
Uso de la política 2821
Información de la política 2821
Versión de la política 2822
Documento de política JSON 2822
Más información 2824
AWSProtonReadOnlyAccess 2824
Uso de la política 2824
Información de la política 2824
Versión de la política 2825
Documento de política JSON 2825
Más información 2826

AWSProtonServiceGitSyncServiceRolePolicy 2826
Uso de la política 2827
Información de la política 2827
Versión de la política 2827
Documento de política JSON 2827
Más información 2828
AWSProtonSyncServiceRolePolicy 2828
Uso de la política 2828
Información de la política 2828
Versión de la política 2829
Documento de política JSON 2829
Más información 2830
AWSPurchaseOrdersServiceRolePolicy 2830
Uso de la política 2830
Información de la política 2830
Versión de la política 2830
Documento de política JSON 2831
Más información 2832
AWSQuickSetupCFGCPacksPermissionsBoundary 2832
Uso de la política 2832
Información de la política 2832
Versión de la política 2832
Documento de política JSON 2833
Más información 2835
AWSQuickSetupDeploymentRolePolicy 2836
Uso de la política 2836
Información de la política 2836
Versión de la política 2836
Documento de política JSON 2836
Más información 2844
AWSQuickSetupDevOpsGuruPermissionsBoundary 2844
Uso de la política 2845
Información de la política 2845
Versión de la política 2845
Documento de política JSON 2845
Más información 2848

AWSQuickSetupDistributorPermissionsBoundary 2848
Uso de la política 2848
Información de la política 2849
Versión de la política 2849
Documento de política JSON 2849
Más información 2855
AWSQuickSetupEnableAREXExecutionPolicy 2855
Uso de la política 2855
Información de la política 2855
Versión de la política 2855
Documento de política JSON 2856
Más información 2857
AWSQuickSetupEnableDHMCExecutionPolicy 2857
Uso de la política 2858
Información de la política 2858
Versión de la política 2858
Documento de política JSON 2858
Más información 2859
AWSQuickSetupJITNADeploymentRolePolicy 2859
Uso de la política 2860
Información de la política 2860
Versión de la política 2860
Documento de política JSON 2860
Más información 2864
AWSQuickSetupManagedInstanceProfileExecutionPolicy 2864
Uso de la política 2864
Información de la política 2864
Versión de la política 2864
Documento de política JSON 2865
Más información 2869
AWSQuickSetupManageJITNAResourcesExecutionPolicy 2869
Uso de la política 2869
Información de la política 2869
Versión de la política 2869
Documento de política JSON 2870
Más información 2872

AWSQuickSetupPatchPolicyBaselineAccess 2872
Uso de la política 2872
Información de la política 2872
Versión de la política 2872
Documento de política JSON 2873
Más información 2873
AWSQuickSetupPatchPolicyDeploymentRolePolicy 2874
Uso de la política 2874
Información de la política 2874
Versión de la política 2874
Documento de política JSON 2874
Más información 2882
AWSQuickSetupPatchPolicyPermissionsBoundary 2883
Uso de la política 2883
Información de la política 2883
Versión de la política 2883
Documento de política JSON 2883
Más información 2891
AWSQuickSetupSchedulerPermissionsBoundary 2892
Uso de la política 2892
Información de la política 2892
Versión de la política 2892
Documento de política JSON 2892
Más información 2895
AWSQuickSetupSSMDeploymentRolePolicy 2896
Uso de la política 2896
Información de la política 2896
Versión de la política 2896
Documento de política JSON 2896
Más información 2905
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 2905
Uso de la política 2905
Información de la política 2905
Versión de la política 2905
Documento de política JSON 2906
Más información 2906

AWSQuickSetupSSMHostMgmtPermissionsBoundary 2907
Uso de la política 2907
Información de la política 2907
Versión de la política 2907
Documento de política JSON 2907
Más información 2913
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 2914
Uso de la política 2914
Información de la política 2914
Versión de la política 2914
Documento de política JSON 2914
Más información 2916
AWSQuickSetupSSMManageResourcesExecutionPolicy 2916
Uso de la política 2916
Información de la política 2916
Versión de la política 2916
Documento de política JSON 2917
Más información 2919
AWSQuickSightAssetBundleExportPolicy 2920
Uso de la política 2920
Información de la política 2920
Versión de la política 2920
Documento de política JSON 2920
Más información 2922
AWSQuickSightAssetBundleImportPolicy 2923
Uso de la política 2923
Información de la política 2923
Versión de la política 2923
Documento de política JSON 2923
Más información 2926
AWSQuicksightAthenaAccess 2926
Uso de la política 2927
Información de la política 2927
Versión de la política 2927
Documento de política JSON 2927
Más información 2929

AWSQuickSightDescribeRDS 2930
Uso de la política 2930
Información de la política 2930
Versión de la política 2930
Documento de política JSON 2930
Más información 2931
AWSQuickSightDescribeRedshift 2931
Uso de la política 2931
Información de la política 2931
Versión de la política 2931
Documento de política JSON 2932
Más información 2932
AWSQuickSightElasticsearchPolicy 2932
Uso de la política 2932
Información de la política 2932
Versión de la política 2933
Documento de política JSON 2933
Más información 2934
AWSQuickSightIoTAnalyticsAccess 2934
Uso de la política 2934
Información de la política 2934
Versión de la política 2935
Documento de política JSON 2935
Más información 2935
AWSQuickSightListIAM 2936
Uso de la política 2936
Información de la política 2936
Versión de la política 2936
Documento de política JSON 2936
Más información 2937
AWSQuicksightOpenSearchPolicy 2937
Uso de la política 2937
Información de la política 2937
Versión de la política 2937
Documento de política JSON 2938
Más información 2939

AWSQuickSightSageMakerPolicy 2939
Uso de la política 2939
Información de la política 2939
Versión de la política 2939
Documento de política JSON 2939
Más información 2941
AWSQuickSightSecretsManagerWriteAccess 2941
Uso de la política 2941
Información de la política 2941
Versión de la política 2941
Documento de política JSON 2942
Más información 2943
AWSQuickSightSecretsManagerWritePolicy 2943
Uso de la política 2943
Información de la política 2943
Versión de la política 2943
Documento de política JSON 2944
Más información 2944
AWSQuickSightTimestreamPolicy 2945
Uso de la política 2945
Información de la política 2945
Versión de la política 2945
Documento de política JSON 2945
Más información 2946
AWSReachabilityAnalyzerServiceRolePolicy 2946
Uso de la política 2946
Información de la política 2946
Versión de la política 2947
Documento de política JSON 2947
Más información 2949
AWSRefactoringToolkitFullAccess 2949
Uso de la política 2950
Información de la política 2950
Versión de la política 2950
Documento de política JSON 2950
Más información 2964

AWSRefactoringToolkitSidecarPolicy 2964
Uso de la política 2964
Información de la política 2964
Versión de la política 2964
Documento de política JSON 2965
Más información 2966
AWSrePostPrivateCloudWatchAccess 2966
Uso de la política 2966
Información de la política 2966
Versión de la política 2966
Documento de política JSON 2967
Más información 2967
AWSRepostSpaceSupportOperationsPolicy 2967
Uso de la política 2967
Información de la política 2968
Versión de la política 2968
Documento de política JSON 2968
Más información 2969
AWSResilienceHubAsssessmentExecutionPolicy 2969
Uso de la política 2969
Información de la política 2969
Versión de la política 2969
Documento de política JSON 2970
Más información 2974
AWSResourceAccessManagerFullAccess 2975
Uso de la política 2975
Información de la política 2975
Versión de la política 2975
Documento de política JSON 2975
Más información 2976
AWSResourceAccessManagerReadOnlyAccess 2976
Uso de la política 2976
Información de la política 2976
Versión de la política 2976
Documento de política JSON 2976
Más información 2977

AWSResourceAccessManagerResourceShareParticipantAccess 2977
Uso de la política 2977
Información de la política 2977
Versión de la política 2978
Documento de política JSON 2978
Más información 2978
AWSResourceAccessManagerServiceRolePolicy 2979
Uso de la política 2979
Información de la política 2979
Versión de la política 2979
Documento de política JSON 2979
Más información 2980
AWSResourceExplorerFullAccess 2980
Uso de la política 2981
Información de la política 2981
Versión de la política 2981
Documento de política JSON 2981
Más información 2982
AWSResourceExplorerOrganizationsAccess 2982
Uso de la política 2982
Información de la política 2982
Versión de la política 2983
Documento de política JSON 2983
Más información 2984
AWSResourceExplorerReadOnlyAccess 2985
Uso de la política 2985
Información de la política 2985
Versión de la política 2985
Documento de política JSON 2985
Más información 2986
AWSResourceExplorerServiceRolePolicy 2986
Uso de la política 2986
Información de la política 2987
Versión de la política 2987
Documento de política JSON 2987
Más información 3003

AWSResourceGroupsReadOnlyAccess 3003
Uso de la política 3003
Información de la política 3003
Versión de la política 3004
Documento de política JSON 3004
Más información 3005
AWSRoboMaker_FullAccess 3005
Uso de la política 3006
Información de la política 3006
Versión de la política 3006
Documento de política JSON 3006
Más información 3007
AWSRoboMakerReadOnlyAccess 3008
Uso de la política 3008
Información de la política 3008
Versión de la política 3008
Documento de política JSON 3008
Más información 3009
AWSRoboMakerServicePolicy 3009
Uso de la política 3009
Información de la política 3009
Versión de la política 3009
Documento de política JSON 3010
Más información 3011
AWSRoboMakerServiceRolePolicy 3011
Uso de la política 3012
Información de la política 3012
Versión de la política 3012
Documento de política JSON 3012
Más información 3013
AWSRolesAnywhereServicePolicy 3014
Uso de la política 3014
Información de la política 3014
Versión de la política 3014
Documento de política JSON 3014
Más información 3015

AWSS3OnOutpostsServiceRolePolicy 3015
Uso de la política 3015
Información de la política 3015
Versión de la política 3016
Documento de política JSON 3016
Más información 3018
AWSSavingsPlansFullAccess 3019
Uso de la política 3019
Información de la política 3019
Versión de la política 3019
Documento de política JSON 3019
Más información 3020
AWSSavingsPlansReadOnlyAccess 3020
Uso de la política 3020
Información de la política 3020
Versión de la política 3020
Documento de política JSON 3021
Más información 3021
AWSSecurityHubFullAccess 3021
Uso de la política 3021
Información de la política 3021
Versión de la política 3022
Documento de política JSON 3022
Más información 3023
AWSSecurityHubOrganizationsAccess 3023
Uso de la política 3023
Información de la política 3023
Versión de la política 3024
Documento de política JSON 3024
Más información 3026
AWSSecurityHubReadOnlyAccess 3026
Uso de la política 3026
Información de la política 3026
Versión de la política 3027
Documento de política JSON 3027
Más información 3027

AWSSecurityHubServiceRolePolicy 3028
Uso de la política 3028
Información de la política 3028
Versión de la política 3028
Documento de política JSON 3028
Más información 3030
AWSSecurityHubV2ServiceRolePolicy 3030
Uso de la política 3031
Información de la política 3031
Versión de la política 3031
Documento de política JSON 3031
Más información 3033
AWSSecurityIncidentResponseCaseFullAccess 3033
Uso de la política 3034
Información de la política 3034
Versión de la política 3034
Documento de política JSON 3034
Más información 3036
AWSSecurityIncidentResponseFullAccess 3036
Uso de la política 3036
Información de la política 3036
Versión de la política 3036
Documento de política JSON 3037
Más información 3039
AWSSecurityIncidentResponseReadOnlyAccess 3039
Uso de la política 3039
Información de la política 3039
Versión de la política 3039
Documento de política JSON 3040
Más información 3040
AWSSecurityIncidentResponseServiceRolePolicy 3041
Uso de la política 3041
Información de la política 3041
Versión de la política 3041
Documento de política JSON 3041
Más información 3042

AWSSecurityIncidentResponseTriageServiceRolePolicy 3042
Uso de la política 3043
Información de la política 3043
Versión de la política 3043
Documento de política JSON 3043
Más información 3045
AWSServiceCatalogAdminFullAccess 3046
Uso de la política 3046
Información de la política 3046
Versión de la política 3046
Documento de política JSON 3046
Más información 3049
AWSServiceCatalogAdminReadOnlyAccess 3049
Uso de la política 3049
Información de la política 3049
Versión de la política 3050
Documento de política JSON 3050
Más información 3051
AWSServiceCatalogAppRegistryFullAccess 3051
Uso de la política 3052
Información de la política 3052
Versión de la política 3052
Documento de política JSON 3052
Más información 3054
AWSServiceCatalogAppRegistryReadOnlyAccess 3055
Uso de la política 3055
Información de la política 3055
Versión de la política 3055
Documento de política JSON 3055
Más información 3056
AWSServiceCatalogAppRegistryServiceRolePolicy 3056
Uso de la política 3056
Información de la política 3056
Versión de la política 3057
Documento de política JSON 3057
Más información 3058

AWSServiceCatalogEndUserFullAccess 3058
Uso de la política 3058
Información de la política 3058
Versión de la política 3059
Documento de política JSON 3059
Más información 3061
AWSServiceCatalogEndUserReadOnlyAccess 3061
Uso de la política 3061
Información de la política 3061
Versión de la política 3062
Documento de política JSON 3062
Más información 3063
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3064
Uso de la política 3064
Información de la política 3064
Versión de la política 3064
Documento de política JSON 3064
Más información 3065
AWSServiceCatalogSyncServiceRolePolicy 3065
Uso de la política 3065
Información de la política 3065
Versión de la política 3066
Documento de política JSON 3066
Más información 3067
AWSServiceRoleForAmazonEKSNodegroup 3067
Uso de la política 3067
Información de la política 3067
Versión de la política 3068
Documento de política JSON 3068
Más información 3073
AWSServiceRoleForAmazonQDeveloper 3073
Uso de la política 3074
Información de la política 3074
Versión de la política 3074
Documento de política JSON 3074
Más información 3075

AWSServiceRoleForAWSTransform 3075
Uso de la política 3075
Información de la política 3075
Versión de la política 3075
Documento de política JSON 3076
Más información 3076
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3076
Uso de la política 3077
Información de la política 3077
Versión de la política 3077
Documento de política JSON 3077
Más información 3077
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3078
Uso de la política 3078
Información de la política 3078
Versión de la política 3078
Documento de política JSON 3078
Más información 3079
AWSServiceRoleForCodeGuru-Profiler 3079
Uso de la política 3079
Información de la política 3079
Versión de la política 3080
Documento de política JSON 3080
Más información 3080
AWSServiceRoleForCodeWhispererPolicy 3080
Uso de la política 3081
Información de la política 3081
Versión de la política 3081
Documento de política JSON 3081
Más información 3083
AWSServiceRoleForEC2ScheduledInstances 3083
Uso de la política 3083
Información de la política 3083
Versión de la política 3084
Documento de política JSON 3084
Más información 3085

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3085
Uso de la política 3085
Información de la política 3085
Versión de la política 3085
Documento de política JSON 3086
Más información 3086
AWSServiceRoleForImageBuilder 3086
Uso de la política 3086
Información de la política 3086
Versión de la política 3087
Documento de política JSON 3087
Más información 3097
AWSServiceRoleForIoTSiteWise 3097
Uso de la política 3097
Información de la política 3097
Versión de la política 3098
Documento de política JSON 3098
Más información 3099
AWSServiceRoleForLogDeliveryPolicy 3099
Uso de la política 3100
Información de la política 3100
Versión de la política 3100
Documento de política JSON 3100
Más información 3101
AWSServiceRoleForMonitronPolicy 3101
Uso de la política 3101
Información de la política 3101
Versión de la política 3101
Documento de política JSON 3102
Más información 3102
AWSServiceRoleForNeptuneGraphPolicy 3102
Uso de la política 3103
Información de la política 3103
Versión de la política 3103
Documento de política JSON 3103
Más información 3104

AWSServiceRoleForPrivateMarketplaceAdminPolicy 3105
Uso de la política 3105
Información de la política 3105
Versión de la política 3105
Documento de política JSON 3105
Más información 3107
AWSServiceRoleForProcurementInsightsPolicy 3107
Uso de la política 3107
Información de la política 3107
Versión de la política 3108
Documento de política JSON 3108
Más información 3108
AWSServiceRoleForSMS 3108
Uso de la política 3109
Información de la política 3109
Versión de la política 3109
Documento de política JSON 3109
Más información 3116
AWSServiceRoleForUserSubscriptions 3116
Uso de la política 3116
Información de la política 3116
Versión de la política 3116
Documento de política JSON 3117
Más información 3117
AWSServiceRolePolicyForBackupReports 3117
Uso de la política 3118
Información de la política 3118
Versión de la política 3118
Documento de política JSON 3118
Más información 3119
AWSServiceRolePolicyForBackupRestoreTesting 3120
Uso de la política 3120
Información de la política 3120
Versión de la política 3120
Documento de política JSON 3120
Más información 3123

AWSServiceRolePolicyForWorkspacesInstances 3123
Uso de la política 3123
Información de la política 3123
Versión de la política 3124
Documento de política JSON 3124
Más información 3125
AWSShieldDRTAccessPolicy 3125
Uso de la política 3125
Información de la política 3125
Versión de la política 3125
Documento de política JSON 3126
Más información 3127
AWSShieldServiceRolePolicy 3127
Uso de la política 3127
Información de la política 3127
Versión de la política 3127
Documento de política JSON 3128
Más información 3128
AWSSocialMessagingServiceRolePolicy 3128
Uso de la política 3128
Información de la política 3129
Versión de la política 3129
Documento de política JSON 3129
Más información 3129
AWSSSMForSAPServiceLinkedRolePolicy 3130
Uso de la política 3130
Información de la política 3130
Versión de la política 3130
Documento de política JSON 3130
Más información 3139
AWSSSMOpsInsightsServiceRolePolicy 3139
Uso de la política 3139
Información de la política 3139
Versión de la política 3139
Documento de política JSON 3140
Más información 3140

AWSSSODirectoryAdministrator 3141
Uso de la política 3141
Información de la política 3141
Versión de la política 3141
Documento de política JSON 3141
Más información 3142
AWSSSODirectoryReadOnly 3142
Uso de la política 3142
Información de la política 3142
Versión de la política 3142
Documento de política JSON 3143
Más información 3143
AWSSSOMasterAccountAdministrator 3143
Uso de la política 3144
Información de la política 3144
Versión de la política 3144
Documento de política JSON 3144
Más información 3146
AWSSSOMemberAccountAdministrator 3146
Uso de la política 3146
Información de la política 3147
Versión de la política 3147
Documento de política JSON 3147
Más información 3148
AWSSSOReadOnly 3148
Uso de la política 3149
Información de la política 3149
Versión de la política 3149
Documento de política JSON 3149
Más información 3150
AWSSSOServiceRolePolicy 3150
Uso de la política 3150
Información de la política 3150
Versión de la política 3151
Documento de política JSON 3151
Más información 3155

AWSStepFunctionsConsoleFullAccess 3155
Uso de la política 3155
Información de la política 3155
Versión de la política 3155
Documento de política JSON 3155
Más información 3156
AWSStepFunctionsFullAccess 3156
Uso de la política 3157
Información de la política 3157
Versión de la política 3157
Documento de política JSON 3157
Más información 3157
AWSStepFunctionsReadOnlyAccess 3158
Uso de la política 3158
Información de la política 3158
Versión de la política 3158
Documento de política JSON 3158
Más información 3159
AWSStorageGatewayFullAccess 3159
Uso de la política 3159
Información de la política 3160
Versión de la política 3160
Documento de política JSON 3160
Más información 3161
AWSStorageGatewayReadOnlyAccess 3161
Uso de la política 3161
Información de la política 3161
Versión de la política 3161
Documento de política JSON 3162
Más información 3162
AWSStorageGatewayServiceRolePolicy 3163
Uso de la política 3163
Información de la política 3163
Versión de la política 3163
Documento de política JSON 3163
Más información 3164

AWSSupplyChainFederationAdminAccess 3164
Uso de la política 3164
Información de la política 3164
Versión de la política 3164
Documento de política JSON 3165
Más información 3170
AWSSupportAccess 3170
Uso de la política 3170
Información de la política 3171
Versión de la política 3171
Documento de política JSON 3171
Más información 3171
AWSSupportAppFullAccess 3172
Uso de la política 3172
Información de la política 3172
Versión de la política 3172
Documento de política JSON 3172
Más información 3173
AWSSupportAppReadOnlyAccess 3173
Uso de la política 3174
Información de la política 3174
Versión de la política 3174
Documento de política JSON 3174
Más información 3174
AWSSupportPlansFullAccess 3175
Uso de la política 3175
Información de la política 3175
Versión de la política 3175
Documento de política JSON 3175
Más información 3176
AWSSupportPlansReadOnlyAccess 3176
Uso de la política 3176
Información de la política 3176
Versión de la política 3177
Documento de política JSON 3177
Más información 3177

AWSSupportServiceRolePolicy 3177
Uso de la política 3178
Información de la política 3178
Versión de la política 3178
Documento de política JSON 3178
Más información 3265
AWSSystemsManagerAccountDiscoveryServicePolicy 3265
Uso de la política 3265
Información de la política 3265
Versión de la política 3265
Documento de política JSON 3265
Más información 3266
AWSSystemsManagerChangeManagementServicePolicy 3266
Uso de la política 3266
Información de la política 3266
Versión de la política 3267
Documento de política JSON 3267
Más información 3269
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3269
Uso de la política 3269
Información de la política 3269
Versión de la política 3269
Documento de política JSON 3270
Más información 3272
AWSSystemsManagerEnableExplorerExecutionPolicy 3272
Uso de la política 3272
Información de la política 3272
Versión de la política 3272
Documento de política JSON 3273
Más información 3274
AWSSystemsManagerForSAPFullAccess 3274
Uso de la política 3274
Información de la política 3274
Versión de la política 3275
Documento de política JSON 3275
Más información 3276

AWSSystemsManagerForSAPReadOnlyAccess 3276
Uso de la política 3276
Información de la política 3276
Versión de la política 3277
Documento de política JSON 3277
Más información 3277
AWSSystemsManagerJustInTimeAccessServicePolicy 3277
Uso de la política 3278
Información de la política 3278
Versión de la política 3278
Documento de política JSON 3278
Más información 3282
AWSSystemsManagerJustInTimeAccessTokenPolicy 3282
Uso de la política 3283
Información de la política 3283
Versión de la política 3283
Documento de política JSON 3283
Más información 3286
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3286
Uso de la política 3286
Información de la política 3286
Versión de la política 3287
Documento de política JSON 3287
Más información 3289
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3290
Uso de la política 3290
Información de la política 3290
Versión de la política 3290
Documento de política JSON 3290
Más información 3294
AWSSystemsManagerNotificationsServicePolicy 3295
Uso de la política 3295
Información de la política 3295
Versión de la política 3295
Documento de política JSON 3295
Más información 3297

AWSSystemsManagerOpsDataSyncServiceRolePolicy 3297
Uso de la política 3297
Información de la política 3297
Versión de la política 3297
Documento de política JSON 3298
Más información 3301
AWSThinkboxAssetServerPolicy 3301
Uso de la política 3301
Información de la política 3302
Versión de la política 3302
Documento de política JSON 3302
Más información 3303
AWSThinkboxAWSPortalAdminPolicy 3303
Uso de la política 3303
Información de la política 3303
Versión de la política 3303
Documento de política JSON 3304
Más información 3313
AWSThinkboxAWSPortalGatewayPolicy 3314
Uso de la política 3314
Información de la política 3314
Versión de la política 3314
Documento de política JSON 3314
Más información 3316
AWSThinkboxAWSPortalWorkerPolicy 3316
Uso de la política 3317
Información de la política 3317
Versión de la política 3317
Documento de política JSON 3317
Más información 3319
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3319
Uso de la política 3319
Información de la política 3320
Versión de la política 3320
Documento de política JSON 3320
Más información 3323

AWSThinkboxDeadlineResourceTrackerAdminPolicy 3323
Uso de la política 3323
Información de la política 3323
Versión de la política 3323
Documento de política JSON 3324
Más información 3330
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3330
Uso de la política 3330
Información de la política 3330
Versión de la política 3330
Documento de política JSON 3331
Más información 3333
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3334
Uso de la política 3334
Información de la política 3334
Versión de la política 3334
Documento de política JSON 3334
Más información 3336
AWSTransferConsoleFullAccess 3336
Uso de la política 3336
Información de la política 3336
Versión de la política 3336
Documento de política JSON 3337
Más información 3338
AWSTransferFullAccess 3338
Uso de la política 3338
Información de la política 3338
Versión de la política 3338
Documento de política JSON 3338
Más información 3339
AWSTransferLoggingAccess 3340
Uso de la política 3340
Información de la política 3340
Versión de la política 3340
Documento de política JSON 3340
Más información 3341

AWSTransferReadOnlyAccess 3341
Uso de la política 3341
Información de la política 3341
Versión de la política 3341
Documento de política JSON 3342
Más información 3342
AWSTrustedAdvisorPriorityFullAccess 3342
Uso de la política 3343
Información de la política 3343
Versión de la política 3343
Documento de política JSON 3343
Más información 3345
AWSTrustedAdvisorPriorityReadOnlyAccess 3345
Uso de la política 3345
Información de la política 3345
Versión de la política 3346
Documento de política JSON 3346
Más información 3347
AWSTrustedAdvisorReportingServiceRolePolicy 3347
Uso de la política 3347
Información de la política 3347
Versión de la política 3348
Documento de política JSON 3348
Más información 3348
AWSTrustedAdvisorServiceRolePolicy 3349
Uso de la política 3349
Información de la política 3349
Versión de la política 3349
Documento de política JSON 3349
Más información 3352
AWSUserNotificationsServiceLinkedRolePolicy 3352
Uso de la política 3353
Información de la política 3353
Versión de la política 3353
Documento de política JSON 3353
Más información 3354

AWSVendorInsightsAssessorFullAccess 3354
Uso de la política 3355
Información de la política 3355
Versión de la política 3355
Documento de política JSON 3355
Más información 3356
AWSVendorInsightsAssessorReadOnly 3356
Uso de la política 3357
Información de la política 3357
Versión de la política 3357
Documento de política JSON 3357
Más información 3358
AWSVendorInsightsVendorFullAccess 3358
Uso de la política 3358
Información de la política 3358
Versión de la política 3358
Documento de política JSON 3359
Más información 3360
AWSVendorInsightsVendorReadOnly 3361
Uso de la política 3361
Información de la política 3361
Versión de la política 3361
Documento de política JSON 3361
Más información 3362
AWSVpcLatticeServiceRolePolicy 3362
Uso de la política 3363
Información de la política 3363
Versión de la política 3363
Documento de política JSON 3363
Más información 3366
AWSVPCS2SVpnServiceRolePolicy 3366
Uso de la política 3366
Información de la política 3366
Versión de la política 3366
Documento de política JSON 3367
Más información 3368

AWSVPCTransitGatewayServiceRolePolicy 3368
Uso de la política 3368
Información de la política 3368
Versión de la política 3368
Documento de política JSON 3369
Más información 3369
AWSVPCVerifiedAccessServiceRolePolicy 3369
Uso de la política 3370
Información de la política 3370
Versión de la política 3370
Documento de política JSON 3370
Más información 3372
AWSWAFConsoleFullAccess 3372
Uso de la política 3372
Información de la política 3372
Versión de la política 3372
Documento de política JSON 3373
Más información 3380
AWSWAFConsoleReadOnlyAccess 3380
Uso de la política 3380
Información de la política 3380
Versión de la política 3381
Documento de política JSON 3381
Más información 3386
AWSWAFFullAccess 3386
Uso de la política 3386
Información de la política 3386
Versión de la política 3386
Documento de política JSON 3387
Más información 3392
AWSWAFReadOnlyAccess 3392
Uso de la política 3392
Información de la política 3392
Versión de la política 3392
Documento de política JSON 3392
Más información 3396

AWSWellArchitectedDiscoveryServiceRolePolicy 3396
Uso de la política 3396
Información de la política 3396
Versión de la política 3396
Documento de política JSON 3397
Más información 3398
AWSWellArchitectedOrganizationsServiceRolePolicy 3398
Uso de la política 3398
Información de la política 3399
Versión de la política 3399
Documento de política JSON 3399
Más información 3400
AWSWickrFullAccess 3400
Uso de la política 3400
Información de la política 3400
Versión de la política 3400
Documento de política JSON 3400
Más información 3401
AWSXrayCrossAccountSharingConfiguration 3401
Uso de la política 3401
Información de la política 3401
Versión de la política 3401
Documento de política JSON 3402
Más información 3403
AWSXRayDaemonWriteAccess 3403
Uso de la política 3403
Información de la política 3403
Versión de la política 3403
Documento de política JSON 3404
Más información 3404
AWSXrayFullAccess 3404
Uso de la política 3405
Información de la política 3405
Versión de la política 3405
Documento de política JSON 3405
Más información 3406

AWSXrayReadOnlyAccess 3406
Uso de la política 3406
Información de la política 3406
Versión de la política 3406
Documento de política JSON 3406
Más información 3407
AWSXrayWriteOnlyAccess 3408
Uso de la política 3408
Información de la política 3408
Versión de la política 3408
Documento de política JSON 3408
Más información 3409
AWSZonalAutoshiftPracticeRunSLRPolicy 3409
Uso de la política 3409
Información de la política 3409
Versión de la política 3410
Documento de política JSON 3410
Más información 3411
AWSZoneGroupAccessManagementServiceRolePolicy 3411
Uso de la política 3411
Información de la política 3411
Versión de la política 3411
Documento de política JSON 3412
Más información 3412
BatchServiceRolePolicy 3412
Uso de la política 3413
Información de la política 3413
Versión de la política 3413
Documento de política JSON 3413
Más información 3419
Billing 3419
Uso de la política 3419
Información de la política 3420
Versión de la política 3420
Documento de política JSON 3420
Más información 3424

CertificateManagerServiceRolePolicy 3424
Uso de la política 3424
Información de la política 3424
Versión de la política 3424
Documento de política JSON 3425
Más información 3425
ClientVPNServiceConnectionsRolePolicy 3425
Uso de la política 3425
Información de la política 3425
Versión de la política 3426
Documento de política JSON 3426
Más información 3426
ClientVPNServiceRolePolicy 3426
Uso de la política 3427
Información de la política 3427
Versión de la política 3427
Documento de política JSON 3427
Más información 3428
CloudFormationStackSetsOrgAdminServiceRolePolicy 3428
Uso de la política 3428
Información de la política 3428
Versión de la política 3429
Documento de política JSON 3429
Más información 3429
CloudFormationStackSetsOrgMemberServiceRolePolicy 3430
Uso de la política 3430
Información de la política 3430
Versión de la política 3430
Documento de política JSON 3430
Más información 3431
CloudFrontFullAccess 3431
Uso de la política 3431
Información de la política 3432
Versión de la política 3432
Documento de política JSON 3432
Más información 3434

CloudFrontReadOnlyAccess 3434
Uso de la política 3434
Información de la política 3434
Versión de la política 3434
Documento de política JSON 3435
Más información 3435
CloudHSMServiceRolePolicy 3436
Uso de la política 3436
Información de la política 3436
Versión de la política 3436
Documento de política JSON 3436
Más información 3437
CloudSearchFullAccess 3437
Uso de la política 3437
Información de la política 3437
Versión de la política 3437
Documento de política JSON 3438
Más información 3438
CloudSearchReadOnlyAccess 3438
Uso de la política 3438
Información de la política 3438
Versión de la política 3439
Documento de política JSON 3439
Más información 3439
CloudTrailEventContext 3440
Uso de la política 3440
Información de la política 3440
Versión de la política 3440
Documento de política JSON 3440
Más información 3442
CloudTrailServiceRolePolicy 3442
Uso de la política 3442
Información de la política 3442
Versión de la política 3443
Documento de política JSON 3443
Más información 3444

CloudWatch-CrossAccountAccess 3445
Uso de la política 3445
Información de la política 3445
Versión de la política 3445
Documento de política JSON 3445
Más información 3446
CloudWatchActionsEC2Access 3446
Uso de la política 3446
Información de la política 3446
Versión de la política 3446
Documento de política JSON 3447
Más información 3447
CloudWatchAgentAdminPolicy 3447
Uso de la política 3447
Información de la política 3448
Versión de la política 3448
Documento de política JSON 3448
Más información 3449
CloudWatchAgentServerPolicy 3449
Uso de la política 3449
Información de la política 3449
Versión de la política 3450
Documento de política JSON 3450
Más información 3451
CloudWatchApplicationInsightsFullAccess 3451
Uso de la política 3451
Información de la política 3451
Versión de la política 3451
Documento de política JSON 3452
Más información 3453
CloudWatchApplicationInsightsReadOnlyAccess 3453
Uso de la política 3453
Información de la política 3453
Versión de la política 3454
Documento de política JSON 3454
Más información 3454

CloudwatchApplicationInsightsServiceLinkedRolePolicy 3454
Uso de la política 3455
Información de la política 3455
Versión de la política 3455
Documento de política JSON 3455
Más información 3466
CloudWatchApplicationSignalsFullAccess 3466
Uso de la política 3466
Información de la política 3466
Versión de la política 3466
Documento de política JSON 3467
Más información 3469
CloudWatchApplicationSignalsReadOnlyAccess 3470
Uso de la política 3470
Información de la política 3470
Versión de la política 3470
Documento de política JSON 3470
Más información 3473
CloudWatchApplicationSignalsServiceRolePolicy 3473
Uso de la política 3473
Información de la política 3473
Versión de la política 3473
Documento de política JSON 3474
Más información 3476
CloudWatchAutomaticDashboardsAccess 3476
Uso de la política 3476
Información de la política 3477
Versión de la política 3477
Documento de política JSON 3477
Más información 3478
CloudWatchCrossAccountSharingConfiguration 3479
Uso de la política 3479
Información de la política 3479
Versión de la política 3479
Documento de política JSON 3479
Más información 3480

CloudWatchEventsBuiltInTargetExecutionAccess 3480
Uso de la política 3481
Información de la política 3481
Versión de la política 3481
Documento de política JSON 3481
Más información 3482
CloudWatchEventsFullAccess 3482
Uso de la política 3482
Información de la política 3482
Versión de la política 3482
Documento de política JSON 3483
Más información 3485
CloudWatchEventsInvocationAccess 3485
Uso de la política 3485
Información de la política 3485
Versión de la política 3485
Documento de política JSON 3486
Más información 3486
CloudWatchEventsReadOnlyAccess 3486
Uso de la política 3486
Información de la política 3486
Versión de la política 3487
Documento de política JSON 3487
Más información 3488
CloudWatchEventsServiceRolePolicy 3488
Uso de la política 3489
Información de la política 3489
Versión de la política 3489
Documento de política JSON 3489
Más información 3490
CloudWatchFullAccess 3490
Uso de la política 3490
Información de la política 3490
Versión de la política 3490
Documento de política JSON 3491
Más información 3492

CloudWatchFullAccessV2 3492
Uso de la política 3492
Información de la política 3492
Versión de la política 3492
Documento de política JSON 3492
Más información 3494
CloudWatchInternetMonitorFullAccess 3494
Uso de la política 3494
Información de la política 3495
Versión de la política 3495
Documento de política JSON 3495
Más información 3497
CloudWatchInternetMonitorReadOnlyAccess 3497
Uso de la política 3497
Información de la política 3497
Versión de la política 3498
Documento de política JSON 3498
Más información 3499
CloudWatchInternetMonitorServiceRolePolicy 3499
Uso de la política 3499
Información de la política 3499
Versión de la política 3499
Documento de política JSON 3500
Más información 3501
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 3501
Uso de la política 3501
Información de la política 3501
Versión de la política 3501
Documento de política JSON 3502
Más información 3502
CloudWatchLambdaInsightsExecutionRolePolicy 3503
Uso de la política 3503
Información de la política 3503
Versión de la política 3503
Documento de política JSON 3503
Más información 3504

CloudWatchLogsCrossAccountSharingConfiguration 3504
Uso de la política 3504
Información de la política 3504
Versión de la política 3505
Documento de política JSON 3505
Más información 3506
CloudWatchLogsFullAccess 3506
Uso de la política 3506
Información de la política 3506
Versión de la política 3506
Documento de política JSON 3507
Más información 3507
CloudWatchLogsReadOnlyAccess 3507
Uso de la política 3508
Información de la política 3508
Versión de la política 3508
Documento de política JSON 3508
Más información 3509
CloudWatchNetworkFlowMonitorAgentPublishPolicy 3509
Uso de la política 3509
Información de la política 3509
Versión de la política 3510
Documento de política JSON 3510
Más información 3510
CloudWatchNetworkFlowMonitorServiceRolePolicy 3510
Uso de la política 3511
Información de la política 3511
Versión de la política 3511
Documento de política JSON 3511
Más información 3512
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 3512
Uso de la política 3513
Información de la política 3513
Versión de la política 3513
Documento de política JSON 3513
Más información 3514

CloudWatchNetworkMonitorServiceRolePolicy 3514
Uso de la política 3514
Información de la política 3514
Versión de la política 3514
Documento de política JSON 3515
Más información 3516
CloudWatchOpenSearchDashboardAccess 3516
Uso de la política 3516
Información de la política 3516
Versión de la política 3517
Documento de política JSON 3517
Más información 3519
CloudWatchOpenSearchDashboardsFullAccess 3519
Uso de la política 3520
Información de la política 3520
Versión de la política 3520
Documento de política JSON 3520
Más información 3527
CloudWatchReadOnlyAccess 3527
Uso de la política 3527
Información de la política 3528
Versión de la política 3528
Documento de política JSON 3528
Más información 3529
CloudWatchSyntheticsFullAccess 3530
Uso de la política 3530
Información de la política 3530
Versión de la política 3530
Documento de política JSON 3530
Más información 3535
CloudWatchSyntheticsReadOnlyAccess 3536
Uso de la política 3536
Información de la política 3536
Versión de la política 3536
Documento de política JSON 3536
Más información 3537

ComprehendDataAccessRolePolicy 3537
Uso de la política 3537
Información de la política 3537
Versión de la política 3538
Documento de política JSON 3538
Más información 3538
ComprehendFullAccess 3538
Uso de la política 3539
Información de la política 3539
Versión de la política 3539
Documento de política JSON 3539
Más información 3540
ComprehendMedicalFullAccess 3540
Uso de la política 3540
Información de la política 3540
Versión de la política 3540
Documento de política JSON 3540
Más información 3541
ComprehendReadOnly 3541
Uso de la política 3541
Información de la política 3541
Versión de la política 3542
Documento de política JSON 3542
Más información 3543
ComputeOptimizerReadOnlyAccess 3543
Uso de la política 3543
Información de la política 3543
Versión de la política 3544
Documento de política JSON 3544
Más información 3545
ComputeOptimizerServiceRolePolicy 3545
Uso de la política 3545
Información de la política 3546
Versión de la política 3546
Documento de política JSON 3546
Más información 3547

ConfigConformsServiceRolePolicy 3548
Uso de la política 3548
Información de la política 3548
Versión de la política 3548
Documento de política JSON 3548
Más información 3551
CostOptimizationHubAdminAccess 3551
Uso de la política 3551
Información de la política 3551
Versión de la política 3552
Documento de política JSON 3552
Más información 3553
CostOptimizationHubReadOnlyAccess 3553
Uso de la política 3553
Información de la política 3554
Versión de la política 3554
Documento de política JSON 3554
Más información 3554
CostOptimizationHubServiceRolePolicy 3555
Uso de la política 3555
Información de la política 3555
Versión de la política 3555
Documento de política JSON 3555
Más información 3557
CustomerProfilesServiceLinkedRolePolicy 3557
Uso de la política 3557
Información de la política 3557
Versión de la política 3557
Documento de política JSON 3557
Más información 3558
DatabaseAdministrator 3559
Uso de la política 3559
Información de la política 3559
Versión de la política 3559
Documento de política JSON 3559
Más información 3562

DataScientist 3562
Uso de la política 3562
Información de la política 3562
Versión de la política 3562
Documento de política JSON 3563
Más información 3566
DAXServiceRolePolicy 3567
Uso de la política 3567
Información de la política 3567
Versión de la política 3567
Documento de política JSON 3567
Más información 3568
DeclarativePoliciesEC2Report 3568
Uso de la política 3568
Información de la política 3568
Versión de la política 3569
Documento de política JSON 3569
Más información 3569
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3570
Uso de la política 3570
Información de la política 3570
Versión de la política 3570
Documento de política JSON 3570
Más información 3571
DynamoDBKinesisReplicationServiceRolePolicy 3571
Uso de la política 3571
Información de la política 3571
Versión de la política 3572
Documento de política JSON 3572
Más información 3572
DynamoDBReplicationServiceRolePolicy 3573
Uso de la política 3573
Información de la política 3573
Versión de la política 3573
Documento de política JSON 3573
Más información 3574

EC2FastLaunchFullAccess 3575
Uso de la política 3575
Información de la política 3575
Versión de la política 3575
Documento de política JSON 3575
Más información 3582
EC2FastLaunchServiceRolePolicy 3582
Uso de la política 3583
Información de la política 3583
Versión de la política 3583
Documento de política JSON 3583
Más información 3588
EC2FleetTimeShiftableServiceRolePolicy 3589
Uso de la política 3589
Información de la política 3589
Versión de la política 3589
Documento de política JSON 3589
Más información 3591
Ec2ImageBuilderCrossAccountDistributionAccess 3591
Uso de la política 3591
Información de la política 3591
Versión de la política 3591
Documento de política JSON 3592
Más información 3592
EC2ImageBuilderLifecycleExecutionPolicy 3592
Uso de la política 3593
Información de la política 3593
Versión de la política 3593
Documento de política JSON 3593
Más información 3595
EC2InstanceConnect 3595
Uso de la política 3595
Información de la política 3596
Versión de la política 3596
Documento de política JSON 3596
Más información 3596

Ec2InstanceConnectEndpoint 3597
Uso de la política 3597
Información de la política 3597
Versión de la política 3597
Documento de política JSON 3597
Más información 3599
EC2InstanceProfileForImageBuilder 3600
Uso de la política 3600
Información de la política 3600
Versión de la política 3600
Documento de política JSON 3600
Más información 3603
EC2InstanceProfileForImageBuilderECRContainerBuilds 3603
Uso de la política 3603
Información de la política 3603
Versión de la política 3604
Documento de política JSON 3604
Más información 3605
ECRReplicationServiceRolePolicy 3605
Uso de la política 3606
Información de la política 3606
Versión de la política 3606
Documento de política JSON 3606
Más información 3607
ECRTemplateServiceRolePolicy 3607
Uso de la política 3607
Información de la política 3607
Versión de la política 3607
Documento de política JSON 3607
Más información 3608
ElastiCacheServiceRolePolicy 3608
Uso de la política 3608
Información de la política 3608
Versión de la política 3609
Documento de política JSON 3609
Más información 3611

ElasticLoadBalancingFullAccess 3611
Uso de la política 3611
Información de la política 3611
Versión de la política 3611
Documento de política JSON 3612
Más información 3613
ElasticLoadBalancingReadOnly 3613
Uso de la política 3613
Información de la política 3613
Versión de la política 3614
Documento de política JSON 3614
Más información 3615
ElementalActivationsDownloadSoftwareAccess 3615
Uso de la política 3615
Información de la política 3615
Versión de la política 3616
Documento de política JSON 3616
Más información 3616
ElementalActivationsFullAccess 3616
Uso de la política 3617
Información de la política 3617
Versión de la política 3617
Documento de política JSON 3617
Más información 3617
ElementalActivationsGenerateLicenses 3618
Uso de la política 3618
Información de la política 3618
Versión de la política 3618
Documento de política JSON 3618
Más información 3619
ElementalActivationsReadOnlyAccess 3619
Uso de la política 3619
Información de la política 3619
Versión de la política 3620
Documento de política JSON 3620
Más información 3620

ElementalAppliancesSoftwareFullAccess 3620
Uso de la política 3621
Información de la política 3621
Versión de la política 3621
Documento de política JSON 3621
Más información 3621
ElementalAppliancesSoftwareReadOnlyAccess 3622
Uso de la política 3622
Información de la política 3622
Versión de la política 3622
Documento de política JSON 3622
Más información 3623
ElementalSupportCenterFullAccess 3623
Uso de la política 3623
Información de la política 3623
Versión de la política 3624
Documento de política JSON 3624
Más información 3624
EMRDescribeClusterPolicyForEMRWAL 3624
Uso de la política 3625
Información de la política 3625
Versión de la política 3625
Documento de política JSON 3625
Más información 3626
FMSServiceRolePolicy 3626
Uso de la política 3626
Información de la política 3626
Versión de la política 3626
Documento de política JSON 3626
Más información 3643
FSxDeleteServiceLinkedRoleAccess 3643
Uso de la política 3643
Información de la política 3643
Versión de la política 3644
Documento de política JSON 3644
Más información 3644

GameLiftContainerFleetPolicy 3644
Uso de la política 3645
Información de la política 3645
Versión de la política 3645
Documento de política JSON 3645
Más información 3646
GameLiftGameServerGroupPolicy 3647
Uso de la política 3647
Información de la política 3647
Versión de la política 3647
Documento de política JSON 3647
Más información 3649
GitLabDuoWithAmazonQPermissionsPolicy 3649
Uso de la política 3649
Información de la política 3649
Versión de la política 3650
Documento de política JSON 3650
Más información 3651
GlobalAcceleratorFullAccess 3651
Uso de la política 3651
Información de la política 3651
Versión de la política 3651
Documento de política JSON 3652
Más información 3653
GlobalAcceleratorReadOnlyAccess 3653
Uso de la política 3653
Información de la política 3653
Versión de la política 3653
Documento de política JSON 3654
Más información 3654
GreengrassOTAUpdateArtifactAccess 3654
Uso de la política 3654
Información de la política 3654
Versión de la política 3655
Documento de política JSON 3655
Más información 3655

GroundTruthSyntheticConsoleFullAccess 3656
Uso de la política 3656
Información de la política 3656
Versión de la política 3656
Documento de política JSON 3656
Más información 3657
GroundTruthSyntheticConsoleReadOnlyAccess 3657
Uso de la política 3657
Información de la política 3657
Versión de la política 3657
Documento de política JSON 3658
Más información 3658
Health_OrganizationsServiceRolePolicy 3658
Uso de la política 3659
Información de la política 3659
Versión de la política 3659
Documento de política JSON 3659
Más información 3660
IAMAccessAdvisorReadOnly 3660
Uso de la política 3660
Información de la política 3660
Versión de la política 3660
Documento de política JSON 3660
Más información 3661
IAMAccessAnalyzerFullAccess 3662
Uso de la política 3662
Información de la política 3662
Versión de la política 3662
Documento de política JSON 3662
Más información 3663
IAMAccessAnalyzerReadOnlyAccess 3663
Uso de la política 3664
Información de la política 3664
Versión de la política 3664
Documento de política JSON 3664
Más información 3665

IAMFullAccess 3665
Uso de la política 3665
Información de la política 3665
Versión de la política 3665
Documento de política JSON 3666
Más información 3666
IAMReadOnlyAccess 3666
Uso de la política 3667
Información de la política 3667
Versión de la política 3667
Documento de política JSON 3667
Más información 3668
IAMSelfManageServiceSpecificCredentials 3668
Uso de la política 3668
Información de la política 3668
Versión de la política 3668
Documento de política JSON 3669
Más información 3669
IAMUserChangePassword 3669
Uso de la política 3669
Información de la política 3670
Versión de la política 3670
Documento de política JSON 3670
Más información 3671
IAMUserSSHKeys 3671
Uso de la política 3671
Información de la política 3671
Versión de la política 3671
Documento de política JSON 3671
Más información 3672
IVSFullAccess 3672
Uso de la política 3672
Información de la política 3672
Versión de la política 3673
Documento de política JSON 3673
Más información 3673

IVSReadOnlyAccess 3674
Uso de la política 3674
Información de la política 3674
Versión de la política 3674
Documento de política JSON 3674
Más información 3675
IVSRecordToS3 3676
Uso de la política 3676
Información de la política 3676
Versión de la política 3676
Documento de política JSON 3676
Más información 3677
KafkaConnectServiceRolePolicy 3677
Uso de la política 3677
Información de la política 3677
Versión de la política 3677
Documento de política JSON 3678
Más información 3679
KafkaServiceRolePolicy 3679
Uso de la política 3679
Información de la política 3680
Versión de la política 3680
Documento de política JSON 3680
Más información 3681
KeyspacesCDCServiceRolePolicy 3682
Uso de la política 3682
Información de la política 3682
Versión de la política 3682
Documento de política JSON 3682
Más información 3683
KeyspacesReplicationServiceRolePolicy 3683
Uso de la política 3683
Información de la política 3683
Versión de la política 3683
Documento de política JSON 3684
Más información 3685

LakeFormationDataAccessServiceRolePolicy 3685
Uso de la política 3685
Información de la política 3685
Versión de la política 3686
Documento de política JSON 3686
Más información 3686
LexBotPolicy 3686
Uso de la política 3687
Información de la política 3687
Versión de la política 3687
Documento de política JSON 3687
Más información 3688
LexChannelPolicy 3688
Uso de la política 3688
Información de la política 3688
Versión de la política 3688
Documento de política JSON 3689
Más información 3689
LightsailExportAccess 3689
Uso de la política 3689
Información de la política 3689
Versión de la política 3690
Documento de política JSON 3690
Más información 3691
MediaConnectGatewayInstanceRolePolicy 3691
Uso de la política 3691
Información de la política 3691
Versión de la política 3691
Documento de política JSON 3692
Más información 3692
MediaPackageServiceRolePolicy 3692
Uso de la política 3692
Información de la política 3693
Versión de la política 3693
Documento de política JSON 3693
Más información 3694

MemoryDBServiceRolePolicy 3694
Uso de la política 3694
Información de la política 3694
Versión de la política 3694
Documento de política JSON 3694
Más información 3697
MigrationHubDMSAccessServiceRolePolicy 3697
Uso de la política 3697
Información de la política 3697
Versión de la política 3697
Documento de política JSON 3698
Más información 3698
MigrationHubServiceRolePolicy 3699
Uso de la política 3699
Información de la política 3699
Versión de la política 3699
Documento de política JSON 3699
Más información 3701
MigrationHubSMSAccessServiceRolePolicy 3701
Uso de la política 3701
Información de la política 3701
Versión de la política 3701
Documento de política JSON 3701
Más información 3702
MonitronServiceRolePolicy 3703
Uso de la política 3703
Información de la política 3703
Versión de la política 3703
Documento de política JSON 3703
Más información 3704
MultiPartyApprovalFullAccess 3704
Uso de la política 3704
Información de la política 3704
Versión de la política 3704
Documento de política JSON 3705
Más información 3706

MultiPartyApprovalReadOnlyAccess 3707
Uso de la política 3707
Información de la política 3707
Versión de la política 3707
Documento de política JSON 3707
Más información 3708
NeptuneConsoleFullAccess 3708
Uso de la política 3709
Información de la política 3709
Versión de la política 3709
Documento de política JSON 3709
Más información 3715
NeptuneFullAccess 3715
Uso de la política 3715
Información de la política 3715
Versión de la política 3715
Documento de política JSON 3716
Más información 3720
NeptuneGraphReadOnlyAccess 3720
Uso de la política 3720
Información de la política 3720
Versión de la política 3720
Documento de política JSON 3721
Más información 3722
NeptuneReadOnlyAccess 3722
Uso de la política 3722
Información de la política 3723
Versión de la política 3723
Documento de política JSON 3723
Más información 3725
NetworkAdministrator 3725
Uso de la política 3726
Información de la política 3726
Versión de la política 3726
Documento de política JSON 3726
Más información 3733

NetworkSecurityDirectorServiceLinkedRolePolicy 3733
Uso de la política 3733
Información de la política 3734
Versión de la política 3734
Documento de política JSON 3734
Más información 3738
OAMFullAccess 3738
Uso de la política 3738
Información de la política 3738
Versión de la política 3738
Documento de política JSON 3738
Más información 3739
OAMReadOnlyAccess 3739
Uso de la política 3739
Información de la política 3739
Versión de la política 3739
Documento de política JSON 3740
Más información 3740
OpensearchIngestionSelfManagedVpcePolicy 3740
Uso de la política 3741
Información de la política 3741
Versión de la política 3741
Documento de política JSON 3741
Más información 3742
PartnerCentralAccountManagementUserRoleAssociation 3742
Uso de la política 3742
Información de la política 3742
Versión de la política 3743
Documento de política JSON 3743
Más información 3744
PowerUserAccess 3744
Uso de la política 3744
Información de la política 3744
Versión de la política 3744
Documento de política JSON 3745
Más información 3745

QAppsServiceRolePolicy 3746
Uso de la política 3746
Información de la política 3746
Versión de la política 3746
Documento de política JSON 3746
Más información 3747
QBusinessQuicksightPluginPolicy 3747
Uso de la política 3747
Información de la política 3747
Versión de la política 3747
Documento de política JSON 3748
Más información 3748
QBusinessServiceRolePolicy 3748
Uso de la política 3748
Información de la política 3749
Versión de la política 3749
Documento de política JSON 3749
Más información 3751
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 3751
Uso de la política 3751
Información de la política 3751
Versión de la política 3751
Documento de política JSON 3752
Más información 3752
RDSCloudHsmAuthorizationRole 3752
Uso de la política 3753
Información de la política 3753
Versión de la política 3753
Documento de política JSON 3753
Más información 3754
ReadOnlyAccess 3754
Uso de la política 3754
Información de la política 3754
Versión de la política 3754
Documento de política JSON 3754
Más información 3810

ResourceGroupsandTagEditorFullAccess 3810
Uso de la política 3810
Información de la política 3811
Versión de la política 3811
Documento de política JSON 3811
Más información 3812
ResourceGroupsandTagEditorReadOnlyAccess 3812
Uso de la política 3812
Información de la política 3812
Versión de la política 3812
Documento de política JSON 3813
Más información 3813
ResourceGroupsServiceRolePolicy 3813
Uso de la política 3814
Información de la política 3814
Versión de la política 3814
Documento de política JSON 3814
Más información 3815
ResourceGroupsTaggingAPITagUntagSupportedResources 3815
Uso de la política 3815
Información de la política 3815
Versión de la política 3815
Documento de política JSON 3816
Más información 3824
ROSAAmazonEBSCSIDriverOperatorPolicy 3824
Uso de la política 3824
Información de la política 3824
Versión de la política 3825
Documento de política JSON 3825
Más información 3828
ROSACloudNetworkConfigOperatorPolicy 3828
Uso de la política 3828
Información de la política 3829
Versión de la política 3829
Documento de política JSON 3829
Más información 3830

ROSAControlPlaneOperatorPolicy 3830
Uso de la política 3830
Información de la política 3830
Versión de la política 3831
Documento de política JSON 3831
Más información 3835
ROSAImageRegistryOperatorPolicy 3835
Uso de la política 3836
Información de la política 3836
Versión de la política 3836
Documento de política JSON 3836
Más información 3837
ROSAIngressOperatorPolicy 3838
Uso de la política 3838
Información de la política 3838
Versión de la política 3838
Documento de política JSON 3838
Más información 3839
ROSAInstallerPolicy 3840
Uso de la política 3840
Información de la política 3840
Versión de la política 3840
Documento de política JSON 3840
Más información 3848
ROSAKMSProviderPolicy 3848
Uso de la política 3849
Información de la política 3849
Versión de la política 3849
Documento de política JSON 3849
Más información 3850
ROSAKubeControllerPolicy 3850
Uso de la política 3850
Información de la política 3850
Versión de la política 3850
Documento de política JSON 3851
Más información 3855

ROSAManageSubscription 3855
Uso de la política 3855
Información de la política 3855
Versión de la política 3856
Documento de política JSON 3856
Más información 3857
ROSANodePoolManagementPolicy 3857
Uso de la política 3857
Información de la política 3857
Versión de la política 3857
Documento de política JSON 3858
Más información 3864
ROSASRESupportPolicy 3864
Uso de la política 3864
Información de la política 3864
Versión de la política 3864
Documento de política JSON 3865
Más información 3869
ROSAWorkerInstancePolicy 3870
Uso de la política 3870
Información de la política 3870
Versión de la política 3870
Documento de política JSON 3870
Más información 3871
Route53RecoveryReadinessServiceRolePolicy 3872
Uso de la política 3872
Información de la política 3872
Versión de la política 3872
Documento de política JSON 3872
Más información 3876
Route53ResolverServiceRolePolicy 3876
Uso de la política 3876
Información de la política 3876
Versión de la política 3876
Documento de política JSON 3877
Más información 3877

S3StorageLensServiceRolePolicy 3877
Uso de la política 3878
Información de la política 3878
Versión de la política 3878
Documento de política JSON 3878
Más información 3879
SageMakerStudioAdminProjectUserRolePolicy 3879
Uso de la política 3879
Información de la política 3879
Versión de la política 3879
Documento de política JSON 3880
Más información 3882
SageMakerStudioBedrockAgentServiceRolePolicy 3882
Uso de la política 3882
Información de la política 3883
Versión de la política 3883
Documento de política JSON 3883
Más información 3886
SageMakerStudioBedrockChatAgentUserRolePolicy 3887
Uso de la política 3887
Información de la política 3887
Versión de la política 3887
Documento de política JSON 3887
Más información 3891
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 3892
Uso de la política 3892
Información de la política 3892
Versión de la política 3892
Documento de política JSON 3892
Más información 3896
SageMakerStudioBedrockFlowServiceRolePolicy 3896
Uso de la política 3896
Información de la política 3896
Versión de la política 3897
Documento de política JSON 3897
Más información 3901

SageMakerStudioBedrockFunctionExecutionRolePolicy 3901
Uso de la política 3901
Información de la política 3901
Versión de la política 3901
Documento de política JSON 3902
Más información 3903
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 3903
Uso de la política 3903
Información de la política 3903
Versión de la política 3903
Documento de política JSON 3904
Más información 3905
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 3905
Uso de la política 3905
Información de la política 3905
Versión de la política 3905
Documento de política JSON 3906
Más información 3909
SageMakerStudioBedrockPromptUserRolePolicy 3909
Uso de la política 3910
Información de la política 3910
Versión de la política 3910
Documento de política JSON 3910
Más información 3913
SageMakerStudioDomainExecutionRolePolicy 3913
Uso de la política 3913
Información de la política 3913
Versión de la política 3913
Documento de política JSON 3914
Más información 3919
SageMakerStudioDomainServiceRolePolicy 3920
Uso de la política 3920
Información de la política 3920
Versión de la política 3920
Documento de política JSON 3920
Más información 3921

SageMakerStudioEMRInstanceRolePolicy 3922
Uso de la política 3922
Información de la política 3922
Versión de la política 3922
Documento de política JSON 3922
Más información 3926
SageMakerStudioEMRServiceRolePolicy 3926
Uso de la política 3926
Información de la política 3926
Versión de la política 3926
Documento de política JSON 3927
Más información 3929
SageMakerStudioFullAccess 3930
Uso de la política 3930
Información de la política 3930
Versión de la política 3930
Documento de política JSON 3930
Más información 3939
SageMakerStudioProjectProvisioningRolePolicy 3940
Uso de la política 3940
Información de la política 3940
Versión de la política 3940
Documento de política JSON 3940
Más información 4008
SageMakerStudioProjectRoleMachineLearningPolicy 4008
Uso de la política 4008
Información de la política 4008
Versión de la política 4008
Documento de política JSON 4009
Más información 4031
SageMakerStudioProjectUserRolePermissionsBoundary 4031
Uso de la política 4031
Información de la política 4031
Versión de la política 4032
Documento de política JSON 4032
Más información 4087

SageMakerStudioProjectUserRolePolicy 4087
Uso de la política 4088
Información de la política 4088
Versión de la política 4088
Documento de política JSON 4088
Más información 4149
SageMakerStudioQueryExecutionRolePolicy 4149
Uso de la política 4150
Información de la política 4150
Versión de la política 4150
Documento de política JSON 4150
Más información 4152
SecretsManagerReadWrite 4152
Uso de la política 4152
Información de la política 4152
Versión de la política 4153
Documento de política JSON 4153
Más información 4154
SecurityAudit 4155
Uso de la política 4155
Información de la política 4155
Versión de la política 4155
Documento de política JSON 4155
Más información 4176
SecurityLakeResourceManagementServiceRolePolicy 4176
Uso de la política 4176
Información de la política 4176
Versión de la política 4177
Documento de política JSON 4177
Más información 4182
SecurityLakeServiceLinkedRole 4182
Uso de la política 4182
Información de la política 4183
Versión de la política 4183
Documento de política JSON 4183
Más información 4186

ServerMigration_ServiceRole 4186
Uso de la política 4186
Información de la política 4186
Versión de la política 4186
Documento de política JSON 4187
Más información 4191
ServerMigrationConnector 4192
Uso de la política 4192
Información de la política 4192
Versión de la política 4192
Documento de política JSON 4192
Más información 4194
ServerMigrationServiceConsoleFullAccess 4194
Uso de la política 4194
Información de la política 4194
Versión de la política 4195
Documento de política JSON 4195
Más información 4196
ServerMigrationServiceLaunchRole 4197
Uso de la política 4197
Información de la política 4197
Versión de la política 4197
Documento de política JSON 4197
Más información 4200
ServerMigrationServiceRoleForInstanceValidation 4200
Uso de la política 4201
Información de la política 4201
Versión de la política 4201
Documento de política JSON 4201
Más información 4202
ServiceQuotasFullAccess 4202
Uso de la política 4202
Información de la política 4202
Versión de la política 4202
Documento de política JSON 4202
Más información 4204

ServiceQuotasReadOnlyAccess 4204
Uso de la política 4205
Información de la política 4205
Versión de la política 4205
Documento de política JSON 4205
Más información 4206
ServiceQuotasServiceRolePolicy 4206
Uso de la política 4207
Información de la política 4207
Versión de la política 4207
Documento de política JSON 4207
Más información 4207
SimpleWorkflowFullAccess 4208
Uso de la política 4208
Información de la política 4208
Versión de la política 4208
Documento de política JSON 4208
Más información 4209
SMSVoiceServiceRolePolicy 4209
Uso de la política 4209
Información de la política 4209
Versión de la política 4209
Documento de política JSON 4210
Más información 4210
SplitCostAllocationDataServiceRolePolicy 4210
Uso de la política 4210
Información de la política 4211
Versión de la política 4211
Documento de política JSON 4211
Más información 4212
SSMQuickSetupRolePolicy 4212
Uso de la política 4212
Información de la política 4212
Versión de la política 4212
Documento de política JSON 4213
Más información 4215

SupportUser 4216
Uso de la política 4216
Información de la política 4216
Versión de la política 4216
Documento de política JSON 4216
Más información 4221
SystemAdministrator 4221
Uso de la política 4222
Información de la política 4222
Versión de la política 4222
Documento de política JSON 4222
Más información 4228
TranslateFullAccess 4228
Uso de la política 4228
Información de la política 4229
Versión de la política 4229
Documento de política JSON 4229
Más información 4230
TranslateReadOnly 4230
Uso de la política 4230
Información de la política 4230
Versión de la política 4230
Documento de política JSON 4230
Más información 4231
ViewOnlyAccess 4231
Uso de la política 4232
Información de la política 4232
Versión de la política 4232
Documento de política JSON 4232
Más información 4241
VMImportExportRoleForAWSConnector 4241
Uso de la política 4241
Información de la política 4242
Versión de la política 4242
Documento de política JSON 4242
Más información 4243

VPCLatticeFullAccess 4243
Uso de la política 4243
Información de la política 4243
Versión de la política 4243
Documento de política JSON 4244
Más información 4246
VPCLatticeReadOnlyAccess 4246
Uso de la política 4246
Información de la política 4246
Versión de la política 4246
Documento de política JSON 4247
Más información 4247
VPCLatticeServicesInvokeAccess 4248
Uso de la política 4248
Información de la política 4248
Versión de la política 4248
Documento de política JSON 4248
Más información 4249
WAFLoggingServiceRolePolicy 4249
Uso de la política 4249
Información de la política 4249
Versión de la política 4249
Documento de política JSON 4250
Más información 4250
WAFRegionalLoggingServiceRolePolicy 4250
Uso de la política 4250
Información de la política 4251
Versión de la política 4251
Documento de política JSON 4251
Más información 4251
WAFV2LoggingServiceRolePolicy 4252
Uso de la política 4252
Información de la política 4252
Versión de la política 4252
Documento de política JSON 4252
Más información 4253

WellArchitectedConsoleFullAccess 4253
Uso de la política 4253
Información de la política 4253
Versión de la política 4254
Documento de política JSON 4254
Más información 4254
WellArchitectedConsoleReadOnlyAccess 4254
Uso de la política 4255
Información de la política 4255
Versión de la política 4255
Documento de política JSON 4255
Más información 4256
WorkLinkServiceRolePolicy 4256
Uso de la política 4256
Información de la política 4256
Versión de la política 4256
Documento de política JSON 4257
Más información 4257
..... mmmmcclviii

¿Qué son las políticas AWS gestionadas?

Una política AWS gestionada es una política independiente creada y administrada por. AWS AWS las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes. Podrá comenzar a asignar de forma más sencilla los permisos adecuados a los usuarios, grupos y roles que si tuviera que escribir políticas.

Tenga en cuenta que es posible que las políticas AWS administradas no otorguen permisos de privilegios mínimos para sus casos de uso específicos, ya que están disponibles para que los usen todos los clientes. AWS Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando se lance un nuevo AWS servicio o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte políticas administradas de AWS en la Guía del usuario de IAM.

Descripción de las páginas de referencia de las políticas

Cada página de referencia de las políticas incluye la siguiente información:

- Uso de esta política : si puede adjuntar la política a usuarios, grupos y roles
- Detalles de la política
  - Tipo: el tipo de política AWS gestionada
    - `AWS managed policy`— Una política AWS gestionada estándar
    - `Job function policy`: política que se alinea con las funciones laborales comunes de la industria
    - `Service-linked role policy`: política que se adjunta a un rol vinculado a servicios que permite a un servicio realizar acciones en su nombre, como the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`: política diseñada para trabajar con roles de servicio, como the section called “AWSControlTowerServiceRolePolicy”

  - Hora de creación: cuándo se creó la política por primera vez
  - Hora de edición: cuándo se editó esta versión de la política
  - ARN: nombre de recurso de Amazon de la política
- Versión de la política: la versión de los permisos otorgados por la política
- Documento de política de JSON: la política de JSON
- Más información: enlaces a la documentación relacionada con las políticas administradas de AWS

Políticas AWS gestionadas en desuso

AWS actualiza periódicamente las políticas AWS gestionadas. En la mayoría de los casos, agregamos permisos a una política. Esto sucede cuando lanzamos un nuevo servicio o característica. Para mejorar la seguridad de las políticas administradas de AWS , a veces reducimos el alcance de las políticas. Cuando eliminamos los permisos de una política, determinamos el estado obsoleto de la política y ponemos a disposición una nueva. Cuando se AWS desaprueba un servicio o una función, también se desaprueba la política AWS gestionada para esa función.

Si recibe una notificación por correo electrónico en la que se indica que una política que está utilizando está descartada, le recomendamos que tome medidas de inmediato. Identifique el cambio en la política y actualice sus flujos de trabajo. Si AWS proporciona una política de reemplazo, planee adjuntarla a todas las identidades afectadas (usuarios, grupos y roles) y luego separe la política obsoleta de esas identidades.

Una política descartada tiene las siguientes características:

- Se ha eliminado de esta guía.
- Los permisos siguen funcionando para todas las identidades asociadas actualmente.
- En las cuentas donde la política está adjunta a una identidad, aparece en la lista de Políticas de la consola de IAM con un icono de advertencia al lado.
- No se puede adjuntar a ninguna identidad nueva. Si la separa de una identidad actual, no puede volver a acoplarla.
- Después de separarla de todas las entidades actuales, ya no es visible.

AWS políticas gestionadas

AWS políticas gestionadas

- AccessAnalyzerServiceRolePolicy
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy
- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess
- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAugmentedAIFullAccess

- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMarketplaceAccess
- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- 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
- AmazonEBSCSIDriverPolicy
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes

- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- 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
- 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
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- 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
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- 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
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess

- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole

- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- 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
- 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
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- 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
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess

- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup

- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBCMDataExportsServiceRolePolicy
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess

- AWSCleanRoomsReadOnlyAccess
- 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
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- 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
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- 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
- 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
- AWSIAMIdentityCenterAllowListForIdentityContext
- 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
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaMSKExecutionRole

- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess

- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- 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
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess

- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSOpsWorks_FullAccess
- AWSOpsWorksCloudWatchLogs
- AWSOpsWorksCMInstanceProfileRole
- AWSOpsWorksCMServiceRole
- AWSOpsWorksInstanceRegistration
- AWSOpsWorksRegisterCLI_EC2
- AWSOpsWorksRegisterCLI_OnPremises
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralFullAccess
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- 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
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy

- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess

- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup

- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- 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
- 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
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess

- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- Billing
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess

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

- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses

- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- 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
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PowerUserAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly

- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy
- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy

- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy
- SageMakerStudioProjectUserRolePermissionsBoundary
- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SecretsManagerReadWrite
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly

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

AccessAnalyzerServiceRolePolicy

Descripción: permitir al Analizador de acceso analizar los metadatos del recurso

`AccessAnalyzerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de diciembre de 2019 a las 17:13 UTC
- Hora editada: 12 de mayo de 2025 a las 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Versión de la política

Versión de la política: v17 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AdministratorAccess

Descripción: Proporciona acceso completo a AWS los servicios y recursos.

`AdministratorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AdministratorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AdministratorAccess-Amplify

Descripción: concede permisos administrativos a la cuenta al tiempo que permite explícitamente el acceso directo a los recursos que necesitan las aplicaciones de Amplify.

`AdministratorAccess-Amplify` es una política administrada de AWS.

Uso de la política

Puede asociar `AdministratorAccess-Amplify` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 19:03 UTC
- Hora de edición: 04 de abril de 2024 a las 20:35 h UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AdministratorAccess-AWSElasticBeanstalk

Descripción: concede permisos administrativos a la cuenta. Permite explícitamente a los desarrolladores y administradores obtener acceso directo a los recursos que necesitan para administrar las aplicaciones de AWS Elastic Beanstalk

`AdministratorAccess-AWSElasticBeanstalk` es una política administrada de AWS.

Uso de la política

Puede asociar `AdministratorAccess-AWSElasticBeanstalk` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de enero de 2021 a las 19:36 UTC
- Hora editada: 11 de diciembre de 2024 a las 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AIOpsAssistantPolicy

Descripción: Proporciona ReadOnly los permisos necesarios para que Amazon AI Operations Assistant analice AWS los recursos de los clientes durante las investigaciones.

`AIOpsAssistantPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AIOpsAssistantPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de diciembre de 2024 a las 16:21 UTC
- Hora editada: 3 de abril de 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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: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: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: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:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "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: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*",
        "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:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "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: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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AIOpsConsoleAdminPolicy

Descripción: Otorga acceso completo al servicio Amazon AI Operations y a los permisos necesarios a través de AWS la consola. También incluye permisos para usar sesiones de consola con reconocimiento de identidad.

`AIOpsConsoleAdminPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AIOpsConsoleAdminPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 2 de diciembre de 2024 a las 23:51 UTC
- Hora editada: 24 de junio de 2025 a las 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AIOpsOperatorAccess

Descripción: Concede acceso a Amazon AI Operations APIs para crear, actualizar y eliminar investigaciones, eventos de investigación y recursos de investigación. También incluye el ReadOnly acceso a todas las operaciones de IA APIs y el uso de sesiones con reconocimiento de identidad.

`AIOpsOperatorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AIOpsOperatorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 2 de diciembre de 2024 a las 23:51 UTC
- Hora editada: 24 de junio de 2025 a las 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AIOpsReadOnlyAccess

Descripción: Otorga ReadOnly permisos al servicio Amazon AI Operations y a los recursos necesarios.

`AIOpsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AIOpsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de diciembre de 2024 a las 23:51 UTC
- Hora editada: 24 de junio de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessDeviceSetup

Descripción: Proporcionar acceso a los AlexaForBusiness servicios de configuración del dispositivo

`AlexaForBusinessDeviceSetup` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessDeviceSetup` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 20 de mayo de 2019 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessFullAccess

Descripción: Otorga acceso total a AlexaForBusiness los recursos y acceso a los relacionados Servicios de AWS

`AlexaForBusinessFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 1 de julio de 2020 a las 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessGatewayExecution

Descripción: Proporcionar acceso a los AlexaForBusiness servicios para la ejecución de la pasarela

`AlexaForBusinessGatewayExecution` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessGatewayExecution` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 30 de noviembre de 2017 a las 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessLifesizeDelegatedAccessPolicy

Descripción: proporcionar acceso a los dispositivos Lifesize AVS

`AlexaForBusinessLifesizeDelegatedAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessLifesizeDelegatedAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de junio de 2020 a las 19:46 UTC
- Hora de edición: 12 de junio de 2020 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessNetworkProfileServicePolicy

Descripción: esta política habilita a Alexa for Business para realizar tareas automatizadas programadas por los perfiles de red.

`AlexaForBusinessNetworkProfileServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de marzo de 2019 a las 00:53 UTC
- Hora de edición: 5 de abril de 2019 a las 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessPolyDelegatedAccessPolicy

Descripción: proporcionar acceso a los dispositivos Poly AVS

`AlexaForBusinessPolyDelegatedAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessPolyDelegatedAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de octubre de 2019 a las 19:48 UTC
- Hora de edición: 16 de octubre de 2019 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AlexaForBusinessReadOnlyAccess

Descripción: Proporcionar acceso de solo lectura a AlexaForBusiness los servicios

`AlexaForBusinessReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AlexaForBusinessReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:47 UTC
- Hora de edición: 20 de noviembre de 2019 a las 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAPIGatewayAdministrator

Descripción: Proporciona acceso completo a create/edit/delete APIs Amazon API Gateway a través de AWS Management Console.

`AmazonAPIGatewayAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAPIGatewayAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:34 UTC
- Hora de edición: 9 de julio de 2015 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAPIGatewayInvokeFullAccess

Descripción: Proporciona acceso completo a la invocación APIs en Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAPIGatewayInvokeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:36 UTC
- Hora de edición: 18 de diciembre de 2018 a las 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAPIGatewayPushToCloudWatchLogs

Descripción: permite a API Gateway enviar registros a la cuenta del usuario.

`AmazonAPIGatewayPushToCloudWatchLogs` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAPIGatewayPushToCloudWatchLogs` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de noviembre de 2015 a las 23:41 UTC
- Hora de edición: 11 de noviembre de 2015 a las 23:41 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppFlowFullAccess

Descripción: Proporciona acceso total a Amazon AppFlow y acceso a AWS los servicios compatibles como origen o destino del flujo (S3 y Redshift). También proporciona acceso a KMS para el cifrado

`AmazonAppFlowFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppFlowFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de junio de 2020 a las 23:30 UTC
- Hora de edición: 28 de febrero de 2022 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppFlowReadOnlyAccess

Descripción: proporciona acceso de solo lectura a los flujos de Amazon Appflow

`AmazonAppFlowReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppFlowReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de junio de 2020 a las 23:26 UTC
- Hora de edición: 28 de febrero de 2022 a las 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppStreamFullAccess

Descripción: Proporciona acceso completo a Amazon AppStream a través de AWS Management Console.

`AmazonAppStreamFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppStreamFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 28 de agosto de 2020 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppStreamPCAAccess

Descripción: Acceso de Amazon AppStream 2.0 a AWS Certificate Manager Private CA en las cuentas de los clientes para la autenticación basada en certificados

`AmazonAppStreamPCAAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppStreamPCAAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de octubre de 2022 a las 17:05 UTC
- Hora de edición: 24 de octubre de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppStreamReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon AppStream a través del AWS Management Console.

`AmazonAppStreamReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppStreamReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de diciembre de 2016 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAppStreamServiceAccess

Descripción: Política predeterminada para el rol de AppStream servicio de Amazon.

`AmazonAppStreamServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAppStreamServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de noviembre de 2016 a las 04:17 UTC
- Hora de edición: 26 de junio de 2020 a las 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAthenaFullAccess

Descripción: proporcionar acceso completo a Amazon Athena y acceso delimitado a las dependencias que se necesitan para permitir las consultas, la escritura de resultados y la administración de datos.

`AmazonAthenaFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAthenaFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2016 a las 16:46 UTC
- Hora editada: 3 de enero de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Versión de la política

Versión de la política: v13 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAugmentedAIFullAccess

Descripción: Proporciona acceso para realizar todas las operaciones, los recursos de Amazon Augmented AI FlowDefinitions, incluidos HumanTaskUis y HumanLoops. No permite el acceso para crear equipos de trabajo FlowDefinitions contra el público.

`AmazonAugmentedAIFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAugmentedAIFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 3 de diciembre de 2019 a las 16:21 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAugmentedAIHumanLoopFullAccess

Descripción: Proporciona acceso para realizar todas las operaciones en ella HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAugmentedAIHumanLoopFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 16:20 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAugmentedAIIntegratedAPIAccess

Descripción: Proporciona acceso para realizar todas las operaciones, los recursos de Amazon Augmented AI FlowDefinitions, incluidos HumanTaskUis y HumanLoops. También proporciona acceso a las operaciones de los servicios que están integrados con Amazon Augmented AI.

`AmazonAugmentedAIIntegratedAPIAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAugmentedAIIntegratedAPIAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de abril de 2020 a las 20:47 UTC
- Hora de edición: 22 de abril de 2020 a las 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAuroraDSQLConsoleFullAccess

Descripción: Proporciona acceso administrativo completo de la consola a Aurora DSQL

`AmazonAuroraDSQLConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAuroraDSQLConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:36 UTC
- Hora editada: 21 de mayo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAuroraDSQLFullAccess

Descripción: Proporciona acceso administrativo completo a Aurora DSQL

`AmazonAuroraDSQLFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAuroraDSQLFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:36 UTC
- Hora editada: 21 de mayo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonAuroraDSQLReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Aurora DSQL

`AmazonAuroraDSQLReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonAuroraDSQLReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:21 UTC
- Hora editada: 14 de mayo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBedrockFullAccess

Descripción: proporciona acceso completo a Amazon Bedrock, así como acceso limitado a los servicios relacionados que este requiere

`AmazonBedrockFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBedrockFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 06 de diciembre de 2023 a las 15:47 h UTC
- Hora editada: 29 de junio de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBedrockLimitedAccess

Descripción: Proporciona acceso limitado a Amazon Bedrock, así como a los servicios relacionados que necesite

`AmazonBedrockLimitedAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBedrockLimitedAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de junio de 2025 a las 22:22 UTC
- Hora editada: 29 de junio de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:ApplyGuardrail",
        "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" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBedrockMarketplaceAccess

Descripción: Proporciona acceso limitado a Amazon Bedrock Marketplace, así como a los servicios relacionados que necesite

`AmazonBedrockMarketplaceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBedrockMarketplaceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de junio de 2025 a las 22:22 UTC
- Hora editada: 29 de junio de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBedrockReadOnly

Descripción: proporciona acceso de solo lectura a Amazon Bedrock

`AmazonBedrockReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBedrockReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 06 de diciembre de 2023 a las 15:48 h UTC
- Hora editada: 4 de diciembre de 2024 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBedrockStudioPermissionsBoundary

Descripción: define los permisos máximos de los roles de IAM que Amazon Bedrock Studio crea para operar los recursos de Amazon Bedrock Studio.

`AmazonBedrockStudioPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBedrockStudioPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 01 de agosto de 2024 a las 00:24 h UTC
- Hora de edición: 01 de agosto de 2024 a las 00:24 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBraketFullAccess

Descripción: Proporciona acceso completo a Amazon Braket a través del SDK AWS Management Console y. También proporciona acceso a servicios relacionados (por ejemplo, S3 o registros).

`AmazonBraketFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBraketFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de agosto de 2020 a las 20:12 UTC
- Hora editada: 11 de abril de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBraketJobsExecutionPolicy

Descripción: Otorga el acceso Servicios de AWS y los recursos necesarios para ejecutar un Amazon Braket Job, incluidos S3, Cloudwatch, IAM y Braket

`AmazonBraketJobsExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonBraketJobsExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 26 de noviembre de 2021 a las 19:34 UTC
- Hora de edición: 28 de noviembre de 2021 a las 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonBraketServiceRolePolicy

Descripción: Permite a Amazon Braket crear y gestionar AWS recursos en su nombre

`AmazonBraketServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de agosto de 2020 a las 17:12 UTC
- Hora de edición: 6 de agosto de 2020 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeFullAccess

Descripción: proporciona acceso completo a la Consola de administración de Amazon Chime a través de AWS Management Console.

`AmazonChimeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonChimeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de noviembre de 2017 a las 22:15 UTC
- Hora de edición: 14 de diciembre de 2020 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeReadOnly

Descripción: proporciona acceso de solo lectura a la Consola de administración de Amazon Chime a través de la AWS Management Console.

`AmazonChimeReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonChimeReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de noviembre de 2017 a las 22:04 UTC
- Hora de edición: 14 de diciembre de 2020 a las 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeSDK

Descripción: proporciona acceso a las operaciones de Amazon Chime SDK

`AmazonChimeSDK` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonChimeSDK` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de febrero de 2020 a las 21:53 UTC
- Hora de edición: 10 de enero de 2023 a las 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Descripción: Política gestionada para el rol vinculado al MediaPipelines servicio Amazon Chime SDK

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de abril de 2022 a las 22:02 UTC
- Hora de edición: 08 de diciembre de 2023 a las 19:14 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeSDKMessagingServiceRolePolicy

Descripción: Permite que Amazon Chime SDK Messaging acceda a AWS los recursos y habilite la funcionalidad de mensajería

`AmazonChimeSDKMessagingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de marzo de 2023 a la 01:43 UTC
- Hora de edición: 3 de marzo de 2023 a la 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeServiceRolePolicy

Descripción: Permite el acceso a AWS los recursos utilizados o administrados por Amazon Chime

`AmazonChimeServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de septiembre de 2019 a las 22:25 UTC
- Hora de edición: 30 de septiembre de 2019 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeTranscriptionServiceLinkedRolePolicy

Descripción: permite a Amazon Chime obtener acceso a Amazon Transcribe y Amazon Transcribe Medical en su nombre

`AmazonChimeTranscriptionServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 4 de agosto de 2021 a las 21:47 UTC
- Hora de edición: 4 de agosto de 2021 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeUserManagement

Descripción: proporciona acceso de administración de usuarios a la Consola de administración de Amazon Chime a través de la AWS Management Console.

`AmazonChimeUserManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonChimeUserManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de noviembre de 2017 a las 22:17 UTC
- Hora de edición: 18 de febrero de 2020 a las 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Descripción: Política gestionada para el rol vinculado a servicios de Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de septiembre de 2019 a las 22:16 UTC
- Hora de edición: 14 de abril de 2023 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudDirectoryFullAccess

Descripción: proporciona acceso completo a Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudDirectoryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de febrero de 2017 a las 00:41 UTC
- Hora de edición: 25 de febrero de 2017 a las 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudDirectoryReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudDirectoryReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de febrero de 2017 a las 23:42 UTC
- Hora de edición: 28 de febrero de 2017 a las 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchEvidentlyFullAccess

Descripción: Proporciona acceso completo únicamente a Amazon CloudWatch Evidently. También proporciona acceso a Amazon S3, Amazon SNS CloudWatch, Amazon y otros servicios relacionados.

`AmazonCloudWatchEvidentlyFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudWatchEvidentlyFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 15:10 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchEvidentlyReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon CloudWatch Evidently

`AmazonCloudWatchEvidentlyReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudWatchEvidentlyReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 15:08 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchEvidentlyServiceRolePolicy

Descripción: Permite a CloudWatch Evidently Service gestionar AWS los recursos asociados en nombre del cliente

`AmazonCloudWatchEvidentlyServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de septiembre de 2022 a las 17:25 UTC
- Hora de edición: 13 de septiembre de 2022 a las 17:25 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchRUMFullAccess

Descripción: Otorga permisos de acceso total al servicio Amazon CloudWatch RUM

`AmazonCloudWatchRUMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudWatchRUMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 15:46 UTC
- Hora de edición: 29 de noviembre de 2021 a las 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchRUMReadOnlyAccess

Descripción: Otorga permisos de solo lectura para el servicio Amazon CloudWatch RUM

`AmazonCloudWatchRUMReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCloudWatchRUMReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 15:43 UTC
- Hora editada: 12 de junio de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCloudWatchRUMServiceRolePolicy

Descripción: Concede permiso a Amazon CloudWatch RUM Service para publicar datos de monitoreo en otros AWS servicios relevantes

`AmazonCloudWatchRUMServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 23:17 UTC
- Hora de edición: 22 de febrero de 2023 a las 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeCatalystFullAccess

Descripción: Proporciona acceso completo a Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeCatalystFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de abril de 2023 a las 16:50 UTC
- Hora de edición: 20 de abril de 2023 a las 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeCatalystReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeCatalystReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de abril de 2023 a las 16:49 UTC
- Hora de edición: 20 de abril de 2023 a las 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeCatalystSupportAccess

Descripción: Permite CodeCatalyst a Amazon crear, actualizar y resolver AWS Support casos en tu nombre.

`AmazonCodeCatalystSupportAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeCatalystSupportAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 12:34 UTC
- Hora de edición: 20 de abril de 2023 a las 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruProfilerAgentAccess

Descripción: Proporciona el acceso requerido por el agente de Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerAgentAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruProfilerAgentAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de febrero de 2021 a las 22:11 UTC
- Hora de edición: 5 de mayo de 2022 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruProfilerFullAccess

Descripción: Proporciona acceso completo a Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruProfilerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 10:13 UTC
- Hora de edición: 15 de julio de 2020 a las 3:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruProfilerReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruProfilerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 10:30 UTC
- Hora de edición: 27 de junio de 2020 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruReviewerFullAccess

Descripción: Otorga acceso total a Amazon CodeGuru Reviewer y acceso limitado a las dependencias requeridas.

`AmazonCodeGuruReviewerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruReviewerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 3 de diciembre de 2019 a las 8:33 UTC
- Hora de edición: 29 de agosto de 2020 a las 4:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruReviewerReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruReviewerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 8:48 UTC
- Hora de edición: 29 de agosto de 2020 a las 4:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruReviewerServiceRolePolicy

Descripción: Un rol vinculado a un servicio necesario para que Amazon CodeGuru Reviewer acceda a los recursos en su nombre.

`AmazonCodeGuruReviewerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 5:31 UTC
- Hora de edición: 27 de noviembre de 2020 a las 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruSecurityFullAccess

Descripción: Proporciona acceso completo a Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruSecurityFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2023 a las 21:03 UTC
- Hora de edición: 9 de mayo de 2023 a las 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCodeGuruSecurityScanAccess

Descripción: Proporciona el acceso necesario para trabajar con escaneos CodeGuru de Amazon Security.

`AmazonCodeGuruSecurityScanAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCodeGuruSecurityScanAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2023 a las 20:54 UTC
- Hora de edición: 09 de mayo de 2023 a las 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoDeveloperAuthenticatedIdentities

Descripción: proporciona acceso a Amazon Cognito APIs para admitir las identidades autenticadas por los desarrolladores desde su backend de autenticación.

`AmazonCognitoDeveloperAuthenticatedIdentities` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCognitoDeveloperAuthenticatedIdentities` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 24 de marzo de 2015 a las 17:22 UTC
- Hora de edición: 24 de marzo de 2015 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:LookupDeveloperIdentity",
```

```
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoIdpEmailServiceRolePolicy

Descripción: permite que el servicio de grupos de usuarios de Amazon Cognito utilice las identidades de SES para enviar correos electrónicos

`AmazonCognitoIdpEmailServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de marzo de 2019 a las 21:32 UTC
- Hora de edición: 21 de marzo de 2019 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoIdpServiceRolePolicy

Descripción: Permite el acceso a los grupos de usuarios de Amazon Cognito Servicios de AWS y los recursos utilizados o gestionados por ellos

`AmazonCognitoIdpServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2020 a las 22:30 UTC
- Hora de edición: 26 de junio de 2020 a las 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoPowerUser

Descripción: proporciona acceso administrativo a los recursos existentes de Amazon Cognito. Necesitará privilegios de Cuenta de AWS administrador para crear nuevos recursos de Cognito.

`AmazonCognitoPowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCognitoPowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de marzo de 2015 a las 17:14 UTC
- Hora editada: 27 de febrero de 2025 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoReadOnly

Descripción: proporciona acceso de solo lectura a los recursos de Amazon Cognito.

`AmazonCognitoReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCognitoReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de marzo de 2015 a las 17:06 UTC

- Hora de edición: 1 de agosto de 2019 a las 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Descripción: esta política define el conjunto de permisos que se permiten a las identidades sin autenticar para los grupos de identidades de Cognito. Esta política no está destinada a utilizarse como una política de permisos independiente. Se utiliza como barrera de protección contra las políticas excesivamente permisivas asociadas a las funciones de un grupo de identidades. No asocie esta política a ningún rol, ya que Cognito Identity Service la incluirá automáticamente como política restringida al crear credenciales. Los privilegios para acceder temporalmente a otros AWS recursos a través del flujo mejorado se definirán ahora mediante la intersección del rol asociado a la identidad del usuario no autenticado proporcionado por un servicio y los privilegios otorgados en esta política administrada que es propiedad de Cognito.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCognitoUnAuthedIdentitiesSessionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de julio de 2023 a las 23:04 UTC
- Hora editada: 1 de noviembre de 2024 a las 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonCognitoUnauthenticatedIdentities

Descripción: esta política define el conjunto de permisos que se permiten a las identidades sin autenticar para los grupos de identidades de Cognito. No es necesario que esté asociado a su rol de unauth, ya que Cognito Identity Service la incluirá automáticamente como una política restringida al crear las credenciales. Los privilegios para acceder temporalmente a otros AWS recursos a través del flujo mejorado se definirán ahora mediante la intersección del rol asociado a la identidad del usuario no autenticado proporcionado por un servicio y los privilegios otorgados en esta política administrada que es propiedad de Cognito.

`AmazonCognitoUnauthenticatedIdentities` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonCognitoUnauthenticatedIdentities` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 1 de febrero de 2023 a las 22:36 UTC
- Hora de edición: 1 de febrero de 2023 a las 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnect_FullAccess

Descripción: El objetivo de esta política es conceder a los usuarios de AWS Connect los permisos necesarios para utilizar los recursos de Connect. Esta política proporciona acceso total a los recursos de AWS Connect a través de Connect Console y de forma pública. APIs

`AmazonConnect_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonConnect_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2020 a las 19:54 UTC
- Hora de edición: 7 de marzo de 2023 a las 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnectCampaignsServiceLinkedRolePolicy

Descripción: política para el rol vinculado al servicio de Campañas de Amazon Connect

`AmazonConnectCampaignsServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de septiembre de 2021 a las 20:54 UTC
- Hora de edición: 03 de octubre de 2024 a las 20:20 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnectReadOnlyAccess

Descripción: Otorga permiso para ver las instancias de Amazon Connect en su Cuenta de AWS.

`AmazonConnectReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonConnectReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de octubre de 2018 a las 21:00 UTC
- Hora de edición: 19 de junio de 2024 a las 15:15 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnectServiceLinkedRolePolicy

Descripción: Permite a Amazon Connect crear y gestionar AWS recursos en su nombre.

`AmazonConnectServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2018 a las 00:21 UTC
- Hora editada: 1 de julio de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v26 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:GetIntegration",
        "profile:PutIntegration",
        "profile:DeleteIntegration",
        "profile:ListEventTriggers",
        "profile:ListSegmentDefinitions",
        "profile:ListProfileAttributeValues",
        "profile:CreateSegmentEstimate",
        "profile:GetSegmentEstimate",
        "profile:BatchGetProfile",
        "profile:BatchGetCalculatedAttributeForProfile",
        "profile:GetSegmentMembership",
        "profile:ListDomainLayouts",
        "profile:CreateUploadJob",
        "profile:ListUploadJobs",
        "profile:DetectProfileObjectType",
        "profile:GetSimilarProfiles"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowCustomerProfilesEventTriggerForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateEventTrigger",
        "profile:GetEventTrigger",
        "profile:UpdateEventTrigger",
        "profile:DeleteEventTrigger"
      ],
      "Resource" : [
```

```
        "arn:aws:profile:*:*:domains/amazon-connect-*/event-triggers/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesDomainLayoutsForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateDomainLayout",
        "profile:UpdateDomainLayout",
        "profile:DeleteDomainLayout",
        "profile:GetDomainLayout"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/layouts/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationImportForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/upload-jobs/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType",
        "profile:ListObjectTypeAttributes"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
```

```
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations",
```

```
        "wisdom:CreateMessageTemplate",
        "wisdom:UpdateMessageTemplate",
        "wisdom:UpdateMessageTemplateMetadata",
        "wisdom:GetMessageTemplate",
        "wisdom:DeleteMessageTemplate",
        "wisdom:ListMessageTemplates",
        "wisdom:SearchMessageTemplates",
        "wisdom:ActivateMessageTemplate",
        "wisdom:DeactivateMessageTemplate",
        "wisdom:CreateMessageTemplateVersion",
        "wisdom:ListMessageTemplateVersions",
        "wisdom:CreateMessageTemplateAttachment",
        "wisdom:DeleteMessageTemplateAttachment",
        "wisdom:RenderMessageTemplate",
        "wisdom:CreateAIAgent",
        "wisdom:CreateAIAgentVersion",
        "wisdom:DeleteAIAgent",
        "wisdom:DeleteAIAgentVersion",
        "wisdom:UpdateAIAgent",
        "wisdom:UpdateAssistantAIAgent",
        "wisdom:RemoveAssistantAIAgent",
        "wisdom:GetAIAgent",
        "wisdom:ListAIAgents",
        "wisdom:ListAIAgentVersions",
        "wisdom:CreateAIPrompt",
        "wisdom:CreateAIPromptVersion",
        "wisdom:DeleteAIPrompt",
        "wisdom:DeleteAIPromptVersion",
        "wisdom:UpdateAIPrompt",
        "wisdom:GetAIPrompt",
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "wisdom:CreateAIGuardrail",
        "wisdom:CreateAIGuardrailVersion",
        "wisdom:DeleteAIGuardrail",
        "wisdom:DeleteAIGuardrailVersion",
        "wisdom:UpdateAIGuardrail",
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:CreateAssistant",
        "wisdom:ListTagsForResource",
        "wisdom:SendMessage",
        "wisdom:GetNextMessage",
```

```
        "wisdom:ListMessages"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateSegmentDefinition",
        "profile:GetSegmentDefinition",
        "profile:DeleteSegmentDefinition",
        "profile:CreateSegmentSnapshot",
        "profile:GetSegmentSnapshot"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/segment-definitions/*"
```

```
      ]
    },
    {
      "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" : "AllowWritePermissionForCustomerProfileObjects",
      "Effect" : "Allow",
```

```
      "Action" : [
        "profile:PutProfileObject"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnectSynchronizationServiceRolePolicy

Descripción: Permite que Amazon Connect sincronice AWS los recursos de todas las regiones en su nombre.

`AmazonConnectSynchronizationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de octubre de 2023 a las 22:38 UTC
- Hora editada: 12 de noviembre de 2024 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:Update*",
        "connect:Delete*",
```

```
        "connect:Describe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonConnectVoiceIDFullAccess

Descripción: proporciona acceso completo a Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonConnectVoiceIDFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de septiembre de 2021 a las 19:04 UTC

- Hora de edición: 26 de septiembre de 2021 a las 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneBedrockModelConsumptionPolicy

Descripción: Proporciona permisos para consumir modelos de Amazon Bedrock, incluida la invocación del perfil de inferencia de la aplicación Amazon Bedrock creado para un dominio de Amazon concreto. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneBedrockModelConsumptionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de noviembre de 2024 a las 22:15 UTC
- Hora editada: 28 de mayo de 2025 a las 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneBedrockModelManagementPolicy

Descripción: Proporciona permisos para administrar el acceso al modelo Amazon Bedrock, incluida la creación, el etiquetado y la eliminación de perfiles de inferencia de aplicaciones.

`AmazonDataZoneBedrockModelManagementPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneBedrockModelManagementPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de noviembre de 2024 a las 22:14 UTC
- Hora editada: 12 de noviembre de 2024 a las 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneDomainExecutionRolePolicy

Descripción: Política predeterminada para el rol DataZone de DomainExecutionRole servicio de Amazon. Amazon utiliza esta función DataZone para catalogar, descubrir, gobernar, compartir y analizar datos en el DataZone dominio de Amazon.

`AmazonDataZoneDomainExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneDomainExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de septiembre de 2023 a las 21:55 UTC
- Hora editada: 3 de diciembre de 2024 a las 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneEnvironmentRolePermissionsBoundary

Descripción: Amazon DataZone crea funciones de IAM para los entornos a fin de realizar acciones de análisis de datos y utiliza esta política al crear estas funciones para definir el límite de sus permisos.

`AmazonDataZoneEnvironmentRolePermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneEnvironmentRolePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de septiembre de 2023 a las 23:38 UTC
- Hora de edición: 17 de noviembre de 2023 a las 23:29 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneFullAccess

Descripción: Proporciona acceso completo a Amazon DataZone a través de los servicios relacionados que requiera, así AWS Management Console como acceso limitado a ellos.

`AmazonDataZoneFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de septiembre de 2023 a las 20:06 UTC
- Hora editada: 22 de mayo de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneFullUserAccess

Descripción: proporciona acceso completo a Amazon DataZone, pero no permite la administración de dominios, usuarios o cuentas asociadas.

`AmazonDataZoneFullUserAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneFullUserAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de septiembre de 2023 a las 21:06 UTC
- Hora editada: 19 de noviembre de 2024 a las 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneGlueManageAccessRolePolicy

Descripción: La política concede permisos que permiten DataZone a Amazon habilitar la publicación y las concesiones de acceso a los datos.

`AmazonDataZoneGlueManageAccessRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneGlueManageAccessRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de septiembre de 2023 a las 20:21 UTC
- Hora editada: 19 de junio de 2025 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZonePortalFullAccessPolicy

Descripción: Proporciona acceso completo a Amazon DataZone APIs

`AmazonDataZonePortalFullAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZonePortalFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de marzo de 2023 a las 18:24 UTC
- Hora de edición: 26 de marzo de 2023 a las 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZonePreviewConsoleFullAccess

Descripción: Proporciona acceso completo a la versión preliminar de Amazon DataZone a través de AWS Management Console. También proporciona acceso selecto a otros servicios relacionados.

`AmazonDataZonePreviewConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZonePreviewConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de marzo de 2023 a las 15:16 UTC
- Hora de edición: 13 de julio de 2023 a las 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneProjectDeploymentPermissionsBoundary

Descripción: Amazon DataZone crea funciones de IAM que utiliza para implementar proyectos de análisis de datos. DataZone utiliza esta política al crear estos roles para definir el límite de sus permisos.

`AmazonDataZoneProjectDeploymentPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneProjectDeploymentPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de marzo de 2023 a las 2:54 UTC
- Hora de edición: 4 de abril de 2023 a las 2:48 UTC

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

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneProjectRolePermissionsBoundary

Descripción: Amazon DataZone crea funciones de IAM para que los proyectos realicen acciones de análisis de datos y utiliza esta política al crear estas funciones para definir el límite de sus permisos.

`AmazonDataZoneProjectRolePermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneProjectRolePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de marzo de 2023 a las 2:51 UTC
- Hora de edición: 21 de marzo de 2023 a las 2:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneRedshiftGlueProvisioningPolicy

Descripción: Amazon DataZone es un servicio de administración de datos que le permite catalogar, descubrir, gobernar, compartir y analizar sus datos. Con Amazon DataZone, puedes compartir tus datos y acceder a ellos en todas las cuentas y regiones compatibles. Amazon DataZone simplifica su experiencia en todos AWS los servicios, incluidos, entre otros, Amazon Redshift, Amazon Athena, AWS Glue y Lake Formation. AWS

`AmazonDataZoneRedshiftGlueProvisioningPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneRedshiftGlueProvisioningPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de septiembre de 2023 a las 20:19 UTC
- Hora de edición: 23 de octubre de 2024 a las 18:29 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneRedshiftManageAccessRolePolicy

Descripción: Esta política otorga a Amazon DataZone permisos para publicar datos de Amazon Redshift en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos publicados en el catálogo de Amazon Redshift o Amazon Redshift Serverless.

`AmazonDataZoneRedshiftManageAccessRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneRedshiftManageAccessRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de septiembre de 2023 a las 20:15 UTC
- Hora de edición: 7 de marzo de 2025 a las 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Descripción: La AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary política es la lista de permisos permitidos en un rol de ejecución creado en un SageMaker entorno aprovisionado por Amazon DataZone.

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de abril de 2024 a las 23:01 h UTC
- Hora editada: 21 de noviembre de 2024 a las 23:06 UTC

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

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
      "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",
        "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",
      "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" : "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" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*",
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "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",
        "elastic-inference:Connect",
        "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneSageMakerManageAccessRolePolicy

Descripción: La AmazonDataZoneSageMakerManageAccessRolePolicy política otorga a Amazon DataZone los permisos necesarios para conceder a los usuarios el acceso a varios recursos del SageMaker entorno.

`AmazonDataZoneSageMakerManageAccessRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneSageMakerManageAccessRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de abril de 2024 a las 23:34 h UTC
- Hora editada: 21 de noviembre de 2024 a las 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDataZoneSageMakerProvisioningRolePolicy

Descripción: La AmazonDataZoneSageMakerProvisioningRolePolicy política otorga a Amazon DataZone los permisos necesarios para interoperar con Amazon SageMaker.

`AmazonDataZoneSageMakerProvisioningRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDataZoneSageMakerProvisioningRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de abril de 2024 a las 23:32 h UTC
- Hora editada: 9 de enero de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDetectiveFullAccess

Descripción: proporciona acceso completo al servicio Amazon Detective y acceso delimitado a las dependencias de la interfaz de usuario de la consola

`AmazonDetectiveFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDetectiveFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de abril de 2020 a las 17:57 UTC
- Hora de edición: 17 de mayo de 2023 a las 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDetectiveInvestigatorAccess

Descripción: proporciona acceso de investigador al servicio de Amazon Detective y acceso delimitado a las dependencias de la interfaz de usuario de la consola. Esta política otorga permiso para acceder a Detective con fines de investigación y acceso limitado por escrito a Guardduty.

`AmazonDetectiveInvestigatorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDetectiveInvestigatorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de enero de 2023 a las 15:24 UTC
- Hora de edición: 27 de noviembre de 2023 a las 03:13 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDetectiveMemberAccess

Descripción: proporciona acceso de miembro al servicio Amazon Detective y acceso delimitado a las dependencias de la interfaz de usuario de la consola.

`AmazonDetectiveMemberAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDetectiveMemberAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de enero de 2023 a las 15:16 UTC
- Hora de edición: 17 de enero de 2023 a las 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDetectiveOrganizationsAccess

Descripción: proporciona a Organizations acceso para administrar el administrador delegado para Amazon Detective y acceso delimitado a las dependencias de la interfaz de usuario de la consola. Esto también concede permiso para crear un rol vinculado al servicio para Detective.

`AmazonDetectiveOrganizationsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDetectiveOrganizationsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de marzo de 2023 a las 15:20 UTC
- Hora de edición: 2 de marzo de 2023 a las 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDetectiveServiceLinkedRolePolicy

Descripción: permite a Amazon Detective realizar llamadas de servicio en su nombre

`AmazonDetectiveServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2021 a las 19:47 UTC
- Hora de edición: 18 de noviembre de 2021 a las 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDevOpsGuruConsoleFullAccess

Descripción: La política otorga acceso completo a la consola de DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDevOpsGuruConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de diciembre de 2021 a las 18:43 UTC

- Hora de edición: 25 de agosto de 2022 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDevOpsGuruFullAccess

Descripción: Proporciona acceso completo a Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDevOpsGuruFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 16:38 UTC
- Hora de edición: 25 de agosto de 2022 a las 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDevOpsGuruOrganizationsAccess

Descripción: Proporcionar acceso para habilitar y administrar Amazon DevOps Guru dentro de una organización.

`AmazonDevOpsGuruOrganizationsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDevOpsGuruOrganizationsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de noviembre de 2021 a las 23:50 UTC
- Hora de edición: 15 de noviembre de 2021 a las 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDevOpsGuruReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDevOpsGuruReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 16:34 UTC
- Hora de edición: 25 de agosto de 2022 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDevOpsGuruServiceRolePolicy

Descripción: Un rol vinculado a un servicio necesario para que Amazon pueda acceder DevOpsGuru a tus recursos.

`AmazonDevOpsGuruServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2020 a las 10:24 UTC
- Hora de edición: 10 de enero de 2023 a las 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDMSCloudWatchLogsRole

Descripción: proporciona acceso para cargar los registros de replicación de DMS en los registros de CloudWatch de la cuenta del cliente.

`AmazonDMSCloudWatchLogsRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDMSCloudWatchLogsRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de enero de 2016 a las 23:44 UTC
- Hora de edición: 23 de mayo de 2023 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDMSRedshiftS3Role

Descripción: proporciona acceso para administrar la configuración de S3 para los puntos de conexión de Redshift para DMS.

`AmazonDMSRedshiftS3Role` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDMSRedshiftS3Role` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2016 a las 17:05 UTC
- Hora de edición: 8 de julio de 2019 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDMSVPCManagementRole

Descripción: Proporciona acceso para administrar la configuración de VPC para las configuraciones de clientes AWS administradas

`AmazonDMSVPCManagementRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDMSVPCManagementRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de noviembre de 2015 a las 16:33 UTC
- Hora de edición: 25 de julio de 2024 a las 15:19 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDB-ElasticServiceRolePolicy

Descripción: Permite que Amazon DocumentDB-Elastic administre AWS los recursos en su nombre.

`AmazonDocDB-ElasticServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2022 a las 14:17 UTC
- Hora de edición: 30 de noviembre de 2022 a las 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDBConsoleFullAccess

Descripción: proporciona acceso completo para administrar Amazon DocumentDB con compatibilidad con MongoDB mediante la AWS Management Console. Tenga en cuenta que esta

política también otorga acceso total para publicar sobre todos los temas de SNS de la cuenta, permisos para crear y editar EC2 instancias de Amazon y configuraciones de VPC, permisos para ver y enumerar claves en Amazon KMS y acceso completo a Amazon RDS y Amazon Neptune.

`AmazonDocDBConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDocDBConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 9 de enero de 2019 a las 20:37 UTC
- Hora editada: 11 de febrero de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDBElasticFullAccess

Descripción: Proporciona acceso completo a los clústeres elásticos de Amazon DocumentDB y a otros permisos necesarios para sus dependencias EC2, incluidos KMS e IAM SecretsManager. CloudWatch

`AmazonDocDBElasticFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDocDBElasticFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 5 de junio de 2023 a las 13:51 UTC
- Hora editada: 11 de febrero de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDBElasticReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon DocDB-Elastic y a las métricas. CloudWatch

`AmazonDocDBElasticReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDocDBElasticReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 8 de junio de 2023 a las 14:37 UTC
- Hora de edición: 21 de junio de 2023 a las 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDBFullAccess

Descripción: proporciona acceso completo a Amazon DocumentDB compatible con MongoDB. Tenga en cuenta que esta política también otorga acceso total a las publicaciones sobre todos los temas de SNS de la cuenta, y brinda acceso total a Amazon RDS y Amazon Neptune.

`AmazonDocDBFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDocDBFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de enero de 2019 a las 20:21 UTC
- Hora de edición: 9 de enero de 2019 a las 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDocDBReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon DocumentDB compatible con MongoDB. Tenga en cuenta que esta política también otorga acceso a los recursos de Amazon RDS y Amazon Neptune.

`AmazonDocDBReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDocDBReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de enero de 2019 a las 20:30 UTC
- Hora de edición: 9 de enero de 2019 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDRSVPCManagement

Descripción: proporciona acceso para administrar la configuración de la VPC para las configuraciones administradas de clientes de Amazon

`AmazonDRSVPCManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDRSVPCManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de septiembre de 2015 a las 00:09 UTC
- Hora de edición: 2 de septiembre de 2015 a las 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDynamoDBFullAccess

Descripción: Proporciona acceso completo a Amazon DynamoDB a través de. AWS Management Console

`AmazonDynamoDBFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDynamoDBFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 29 de enero de 2021 a las 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDynamoDBFullAccess_v2

Descripción: Proporciona acceso completo a Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDynamoDBFullAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de mayo de 2025 a las 14:52 UTC
- Hora editada: 22 de mayo de 2025 a las 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDynamoDBFullAccesswithDataPipeline

Descripción: esta política está en proceso de quedar obsoleta. Consulte la documentación para obtener orientación: https://docs.aws.amazon.com/amazondynamodb/ latest/developerguide/ DynamoDBPipeline.html. Provides full access to Amazon DynamoDB including Export/Import uso de AWS Data Pipeline a través del AWS Management Console.

`AmazonDynamoDBFullAccesswithDataPipeline` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDynamoDBFullAccesswithDataPipeline` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 12 de noviembre de 2015 a las 2:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonDynamoDBReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon DynamoDB a través de. AWS Management Console

`AmazonDynamoDBReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonDynamoDBReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 18 de noviembre de 2024 a las 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEBSCSIDriverPolicy

Descripción: Política de IAM que permite a la cuenta del servicio de conductores de CSI realizar llamadas a servicios relacionados, por ejemplo, EC2 en su nombre.

`AmazonEBSCSIDriverPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEBSCSIDriverPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de abril de 2022 a las 17:24 UTC
- Hora editada: 13 de enero de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "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"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume"
      ],
      "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"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerRegistryFullAccess

Descripción: proporciona acceso administrativo a los recursos de Amazon ECR

`AmazonEC2ContainerRegistryFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerRegistryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de diciembre de 2015 a las 17:06 UTC
- Hora de edición: 5 de diciembre de 2020 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerRegistryPowerUser

Descripción: Proporciona acceso completo a los repositorios de Amazon EC2 Container Registry, pero no permite la eliminación de repositorios ni los cambios de política.

`AmazonEC2ContainerRegistryPowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerRegistryPowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de diciembre de 2015 a las 17:05 UTC
- Hora de edición: 10 de diciembre de 2019 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerRegistryPullOnly

Descripción: Proporciona acceso para extraer imágenes de los repositorios de Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryPullOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerRegistryPullOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 04 de octubre de 2024 a las 16:58 h UTC
- Hora de edición: 04 de octubre de 2024 a las 16:58 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerRegistryReadOnly

Descripción: Proporciona acceso de solo lectura a los repositorios de Amazon EC2 Container Registry.

`AmazonEC2ContainerRegistryReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerRegistryReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 21 de diciembre de 2015 a las 17:04 UTC
- Hora de edición: 10 de diciembre de 2019 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerServiceAutoscaleRole

Descripción: Política para habilitar el escalado automático de tareas para Amazon EC2 Container Service

`AmazonEC2ContainerServiceAutoscaleRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerServiceAutoscaleRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de mayo de 2016 a las 23:25 UTC
- Hora de edición: 5 de febrero de 2018 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerServiceEventsRole

Descripción: Política para habilitar CloudWatch Events for EC2 Container Service

`AmazonEC2ContainerServiceEventsRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerServiceEventsRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de mayo de 2017 a las 16:51 UTC
- Hora de edición: 6 de marzo de 2023 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerServiceforEC2Role

Descripción: Política predeterminada para el EC2 rol de Amazon en Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerServiceforEC2Role` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de marzo de 2015 a las 18:45 UTC
- Hora de edición: 06 de marzo de 2023 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ContainerServiceRole

Descripción: política predeterminada para el rol de servicio de Amazon ECS.

`AmazonEC2ContainerServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ContainerServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 16:14 UTC
- Hora de edición: 11 de agosto de 2016 a las 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2FullAccess

Descripción: Proporciona acceso completo a Amazon EC2 a través de AWS Management Console.

`AmazonEC2FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2018 a las 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2ReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon EC2 a través del AWS Management Console.

`AmazonEC2ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 27 de diciembre de 2024 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2RoleforAWSCodeDeploy

Descripción: Proporciona EC2 acceso al depósito de S3 para descargar la revisión. El CodeDeploy agente necesita esta función en las EC2 instancias.

`AmazonEC2RoleforAWSCodeDeploy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2RoleforAWSCodeDeploy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de mayo de 2015 a las 18:10 UTC
- Hora de edición: 20 de marzo de 2017 a las 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2RoleforAWSCodeDeployLimited

Descripción: Proporciona acceso EC2 limitado al depósito de S3 para descargar la revisión. El CodeDeploy agente necesita esta función en las EC2 instancias.

`AmazonEC2RoleforAWSCodeDeployLimited` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2RoleforAWSCodeDeployLimited` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de agosto de 2020 a las 17:55 UTC
- Hora de edición: 20 de enero de 2022 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2RoleforDataPipelineRole

Descripción: Política predeterminada para el EC2 rol de servicio Amazon Role for Data Pipeline.

`AmazonEC2RoleforDataPipelineRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2RoleforDataPipelineRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 22 de febrero de 2016 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2RoleforSSM

Descripción: esta política quedará obsoleta pronto. Utilice la SSMManaged InstanceCore política de Amazon para habilitar la funcionalidad principal del servicio AWS Systems Manager en EC2 las instancias. Para obtener más información, consulta https://docs.aws.amazon.com/systems-manager/latest/userguide/setup -instance-profile.html

`AmazonEC2RoleforSSM` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2RoleforSSM` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de mayo de 2015 a las 17:48 UTC
- Hora de edición: 24 de enero de 2019 a las 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2RolePolicyForLaunchWizard

Descripción: Política gestionada para el rol de LaunchWizard servicio de Amazon para EC2

`AmazonEC2RolePolicyForLaunchWizard` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2RolePolicyForLaunchWizard` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2019 a las 08:05 UTC
- Hora de edición: 25 de septiembre de 2024 a las 22:40 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2SpotFleetAutoscaleRole

Descripción: Política para habilitar el escalado automático para Amazon EC2 Spot Fleet

`AmazonEC2SpotFleetAutoscaleRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2SpotFleetAutoscaleRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de agosto de 2016 a las 18:27 UTC
- Hora de edición: 18 de febrero de 2019 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEC2SpotFleetTaggingRole

Descripción: Permite que EC2 Spot Fleet solicite, cancele y etiquete instancias puntuales en su nombre.

`AmazonEC2SpotFleetTaggingRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEC2SpotFleetTaggingRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de junio de 2017 a las 18:19 UTC
- Hora de edición: 23 de abril de 2020 a las 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECS_FullAccess

Descripción: Proporciona acceso administrativo a los recursos de Amazon ECS y habilita las funciones de ECS mediante el acceso a otros recursos de AWS servicio VPCs, incluidos los grupos y CloudFormation pilas de Auto Scaling.

`AmazonECS_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonECS_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de noviembre de 2017 a las 21:36 UTC
- Hora de edición: 13 de agosto de 2024 a las 19:39 h UTC

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

Versión de la política

Versión de la política: v21 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSComputeServiceRolePolicy

Descripción: Política que permite a Amazon ECS Compute gestionar sus EC2 instancias y los recursos relacionados como parte de las instancias gestionadas por ECS

`AmazonECSComputeServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de marzo de 2025 a las 17:37 UTC
- Hora editada: 28 de marzo de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Descripción: Proporciona acceso administrativo a Private Certificate Authority, AWS Secrets Manager y otros elementos Servicios de AWS necesarios para administrar las funciones TLS de ECS Service Connect en su nombre.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de enero de 2024 a las 20:08 h UTC
- Hora de edición: 19 de enero de 2024 a las 20:08 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSInfrastructureRolePolicyForVolumes

Descripción: Proporciona acceso a otros recursos de AWS servicio necesarios para administrar en su nombre los volúmenes asociados a las cargas de trabajo de ECS.

`AmazonECSInfrastructureRolePolicyForVolumes` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonECSInfrastructureRolePolicyForVolumes` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de enero de 2024 a las 22:56 h UTC
- Hora de edición: 28 de mayo de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSInfrastructureRolePolicyForVpcLattice

Descripción: Proporciona acceso a otros recursos de AWS servicio necesarios para administrar la función VPC Lattice en las cargas de trabajo de ECS en su nombre.

`AmazonECSInfrastructureRolePolicyForVpcLattice` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonECSInfrastructureRolePolicyForVpcLattice` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 20:02 UTC
- Hora editada: 15 de noviembre de 2024 a las 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSServiceRolePolicy

Descripción: política para permitir a Amazon ECS administrar el clúster.

`AmazonECSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de octubre de 2017 a la 01:18 UTC
- Hora editada: 24 de junio de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "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"
      ],
      "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" : "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonECSTaskExecutionRolePolicy

Descripción: Proporciona acceso a otros recursos AWS de servicio necesarios para ejecutar las tareas de Amazon ECS

`AmazonECSTaskExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonECSTaskExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2017 a las 18:48 UTC
- Hora de edición: 16 de noviembre de 2017 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEFSCSIDriverPolicy

Descripción: Proporciona acceso de administración a los recursos de EFS y acceso de lectura a EC2

`AmazonEFSCSIDriverPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEFSCSIDriverPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 25 de julio de 2023 a las 20:10 UTC
- Hora de edición: 25 de julio de 2023 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKS_CNI_Policy

Descripción: Esta política proporciona al complemento CNI de Amazon VPC (amazon-vpc-cni-k8s) los permisos que necesita para modificar la configuración de la dirección IP en los nodos de trabajo de EKS. Este conjunto de permisos permite al CNI enumerar, describir y modificar las interfaces de Elastic Network en su nombre. Puede encontrar más información sobre el complemento CNI de AWS VPC aquí: 8s https://github.com/aws/ amazon-vpc-cni-k

`AmazonEKS_CNI_Policy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKS_CNI_Policy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de mayo de 2018 a las 21:07 UTC
- Hora de edición: 04 de marzo de 2024 a las 20:20 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSBlockStoragePolicy

Descripción: Política adjunta al rol de clúster de EKS que otorga permisos para administrar los recursos de almacenamiento en bloque del clúster.

`AmazonEKSBlockStoragePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSBlockStoragePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de octubre de 2024 a las 20:18 UTC
- Hora editada: 30 de octubre de 2024 a las 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSClusterPolicy

Descripción: esta política proporciona a Kubernetes los permisos que necesita para administrar recursos en su nombre. Kubernetes requiere CreateTags permisos Ec2: para colocar información de identificación en los EC2 recursos, incluidos, entre otros, las instancias, los grupos de seguridad y las interfaces de red elásticas.

`AmazonEKSClusterPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSClusterPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de mayo de 2018 a las 21:06 UTC
- Hora editada: 17 de abril de 2025 a las 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSComputePolicy

Descripción: Política adjunta al rol de clúster de EKS que otorga permisos para administrar los recursos informáticos del clúster.

`AmazonEKSComputePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSComputePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de noviembre de 2024 a las 21:46 UTC
- Hora editada: 20 de junio de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSConnectorServiceRolePolicy

Descripción: Esta política permite a Amazon EKS gestionar AWS los recursos del conector EKS

`AmazonEKSConnectorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de septiembre de 2021 a las 20:31 UTC
- Hora de edición: 4 de septiembre de 2021 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
          "events:source" : "aws.ssm"
        }
      }
    },
```

```
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSDashboardConsoleReadOnly

Descripción: Proporciona acceso de solo lectura para ver el panel de control en la consola de Amazon EKS. El panel agrega información sobre varios clústeres y recursos relacionados mediante AWS Organizations.

`AmazonEKSDashboardConsoleReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSDashboardConsoleReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de junio de 2025 a las 17:22 UTC
- Hora editada: 19 de junio de 2025 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSDashboardServiceRolePolicy

Descripción: Esta política permite al Amazon EKS Dashboard acceder a la información de toda la organización y mostrarla. La política permite que el servicio EKS Dashboard recopile información sobre la estructura AWS y las cuentas de su Organización.

`AmazonEKSDashboardServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de mayo de 2025 a las 19:07 UTC
- Hora editada: 8 de mayo de 2025, 19:07 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSFargatePodExecutionRolePolicy

Descripción: Proporciona acceso a otros recursos AWS de servicio necesarios para ejecutar los pods de Amazon EKS en AWS Fargate

`AmazonEKSFargatePodExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSFargatePodExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 22 de noviembre de 2019 a las 04:34 UTC
- Hora de edición: 22 de noviembre de 2019 a las 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSForFargateServiceRolePolicy

Descripción: esta política concede los permisos necesarios a Amazon EKS para ejecutar tareas de Fargate

`AmazonEKSForFargateServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de noviembre de 2019 a las 04:36 UTC
- Hora de edición: 22 de noviembre de 2019 a las 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSLoadBalancingPolicy

Descripción: Política adjunta al rol de clúster de EKS que otorga permisos para administrar los recursos de equilibrio de carga del clúster.

`AmazonEKSLoadBalancingPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSLoadBalancingPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de octubre de 2024 a las 20:18 UTC
- Hora editada: 9 de enero de 2025 a las 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${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"
      ],
      "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"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:DeleteProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "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"
      ],
      "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"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSLocalOutpostClusterPolicy

Descripción: esta política proporciona permisos a las instancias del plano de control del clúster local de EKS que se ejecutan en la cuenta para administrar recursos en su nombre.

`AmazonEKSLocalOutpostClusterPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSLocalOutpostClusterPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de agosto de 2022 a las 21:56 UTC
- Hora de edición: 24 de octubre de 2024 a las 17:59 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSLocalOutpostServiceRolePolicy

Descripción: Permite a Amazon EKS Local llamar a AWS los servicios en su nombre.

`AmazonEKSLocalOutpostServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de agosto de 2022 a las 21:53 UTC
- Hora editada: 26 de junio de 2025 a las 18:22 UTC

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

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSNetworkingPolicy

Descripción: Política adjunta al rol de clúster de EKS que otorga permisos para administrar los recursos de red del clúster.

`AmazonEKSNetworkingPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSNetworkingPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de octubre de 2024 a las 22:34 UTC
- Hora editada: 28 de octubre de 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSServicePolicy

Descripción: esta política permite a Amazon Elastic Container Service para Kubernetes crear y administrar los recursos necesarios para operar clústeres de EKS.

`AmazonEKSServicePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSServicePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2018 a las 21:08 UTC
- Hora de edición: 14 de octubre de 2024 a las 21:12 h UTC

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

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSServiceRolePolicy

Descripción: Se requiere un rol vinculado a un servicio para que Amazon EKS pueda llamar a AWS los servicios en su nombre.

`AmazonEKSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de febrero de 2020 a las 20:10 UTC
- Hora editada: 20 de junio de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStores",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "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"
          ]
        }
      }
    },
    {
      "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:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "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:DeregisterTargets",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup",
        "shield:DescribeProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSVPCResourceController

Descripción: Política utilizada por el controlador de recursos de VPC para administrar el ENI y IPs los nodos de trabajo.

`AmazonEKSVPCResourceController` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSVPCResourceController` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de agosto de 2020 a las 00:55 UTC
- Hora de edición: 12 de agosto de 2020 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSWorkerNodeMinimalPolicy

Descripción: esta política permite que los nodos de trabajo de Amazon EKS se conecten a los clústeres de Amazon EKS.

`AmazonEKSWorkerNodeMinimalPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSWorkerNodeMinimalPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 02 de octubre de 2024 a las 20:03 h UTC
- Hora de edición: 02 de octubre de 2024 a las 20:03 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEKSWorkerNodePolicy

Descripción: esta política permite que los nodos de trabajo de Amazon EKS se conecten a los clústeres de Amazon EKS.

`AmazonEKSWorkerNodePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEKSWorkerNodePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2018 a las 21:09 UTC
- Hora de edición: 27 de noviembre de 2023 a las 00:06 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElastiCacheFullAccess

Descripción: Proporciona acceso completo a Amazon ElastiCache a través de AWS Management Console.

`AmazonElastiCacheFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElastiCacheFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 28 de noviembre de 2023 a las 03:49 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElastiCacheReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon ElastiCache a través del AWS Management Console.

`AmazonElastiCacheReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElastiCacheReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticContainerRegistryPublicFullAccess

Descripción: proporciona acceso administrativo a los recursos públicos de Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticContainerRegistryPublicFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 17:25 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticContainerRegistryPublicPowerUser

Descripción: proporciona acceso completo a los repositorios públicos de Amazon ECR, pero no permite eliminar repositorios ni realizar cambios en las políticas.

`AmazonElasticContainerRegistryPublicPowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticContainerRegistryPublicPowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 16:16 UTC
- Hora de edición: 1 de diciembre de 2020 a las 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticContainerRegistryPublicReadOnly

Descripción: proporciona acceso de solo lectura a los repositorios públicos de Amazon ECR.

`AmazonElasticContainerRegistryPublicReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticContainerRegistryPublicReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 17:27 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemClientFullAccess

Descripción: proporciona acceso de cliente raíz a un sistema de archivos de Amazon EFS

`AmazonElasticFileSystemClientFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemClientFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de enero de 2020 a las 16:27 UTC
- Hora de edición: 13 de enero de 2020 a las 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemClientReadOnlyAccess

Descripción: proporciona acceso de cliente de solo lectura a un sistema de archivos de Amazon EFS

`AmazonElasticFileSystemClientReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemClientReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de enero de 2020 a las 16:24 UTC
- Hora de edición: 13 de enero de 2020 a las 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemClientReadWriteAccess

Descripción: proporciona acceso de cliente de lectura y escritura a un sistema de archivos de Amazon EFS

`AmazonElasticFileSystemClientReadWriteAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemClientReadWriteAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de enero de 2020 a las 16:21 UTC
- Hora de edición: 13 de enero de 2020 a las 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemFullAccess

Descripción: Proporciona acceso completo a Amazon EFS a través del AWS Management Console.

`AmazonElasticFileSystemFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 27 de mayo de 2015 a las 16:22 UTC
- Hora editada: 7 de noviembre de 2024 a las 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon EFS a través del AWS Management Console.

`AmazonElasticFileSystemReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2015 a las 16:25 UTC

- Hora editada: 7 de noviembre de 2024 a las 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemServiceRolePolicy

Descripción: Permite a Amazon Elastic File System gestionar AWS los recursos en su nombre

`AmazonElasticFileSystemServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de noviembre de 2019 a las 16:52 UTC
- Hora editada: 7 de noviembre de 2024 a las 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticFileSystemsUtils

Descripción: Permite a los clientes utilizar AWS Systems Manager para gestionar automáticamente el paquete de utilidades de Amazon EFS (amazon-efs-utils) en sus EC2 instancias y utilizarlo CloudWatchLog para recibir notificaciones de éxito o error al montar el sistema de archivos EFS.

`AmazonElasticFileSystemsUtils` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticFileSystemsUtils` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 29 de septiembre de 2020 a las 15:16 UTC
- Hora de edición: 29 de septiembre de 2020 a las 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceEditorsRole

Descripción: Política predeterminada para el rol de servicio de Amazon Elastic MapReduce Editors.

`AmazonElasticMapReduceEditorsRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceEditorsRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2018, 21:55 UTC
- Hora de edición: 09 de febrero de 2023 a las 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceforAutoScalingRole

Descripción: Amazon Elastic MapReduce para Auto Scaling. Rol para permitir que el escalado automático añada y elimine instancias de su clúster de EMR.

`AmazonElasticMapReduceforAutoScalingRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceforAutoScalingRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de noviembre de 2016 a las 01:09 UTC
- Hora de edición: 18 de noviembre de 2016 a las 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceforEC2Role

Descripción: Política predeterminada para el rol Amazon Elastic MapReduce for EC2 Service.

`AmazonElasticMapReduceforEC2Role` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceforEC2Role` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 11 de agosto de 2017 a las 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceFullAccess

Descripción: esta política está en proceso de quedar obsoleta. Consulte la documentación para obtener orientación: https://docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Proporciona acceso completo a Amazon Elastic MapReduce y a los servicios subyacentes que requiere, como EC2 S3

`AmazonElasticMapReduceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 11 de octubre de 2019 a las 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReducePlacementGroupPolicy

Descripción: Política que permite a EMR crear, describir y eliminar grupos de EC2 ubicación.

`AmazonElasticMapReducePlacementGroupPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReducePlacementGroupPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de septiembre de 2020 a las 00:37 UTC
- Hora de edición: 29 de septiembre de 2020 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon Elastic MapReduce a través de AWS Management Console.

`AmazonElasticMapReduceReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 29 de julio de 2020 a las 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticMapReduceRole

Descripción: esta política está en proceso de quedar obsoleta. Consulte la documentación para obtener orientación: https://docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Política predeterminada para el rol de MapReduce servicio de Amazon Elastic.

`AmazonElasticMapReduceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticMapReduceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de junio de 2020 a las 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticsearchServiceRolePolicy

Descripción: Permita que Amazon Elasticsearch Service acceda a otros AWS servicios, como las EC2 redes APIs , en su nombre.

`AmazonElasticsearchServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de julio de 2017 a las 00:15 UTC
- Hora de edición: 23 de octubre de 2023 a las 06:58 UTC

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

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticTranscoder_FullAccess

Descripción: concede a los usuarios acceso completo a Elastic Transcoder, así como el acceso a los servicios asociados que se necesita para la funcionalidad completa de Elastic Transcoder.

`AmazonElasticTranscoder_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticTranscoder_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de abril de 2018 a las 18:59 UTC
- Hora de edición: 10 de junio de 2019 a las 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticTranscoder_JobsSubmitter

Descripción: concede a los usuarios permiso para cambiar ajustes preestablecidos, enviar trabajos y ver la configuración de Elastic Transcoder. Esta política también otorga acceso de solo lectura a algunos otros servicios necesarios para usar la consola de Elastic Transcode, como S3, IAM y SNS.

`AmazonElasticTranscoder_JobsSubmitter` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticTranscoder_JobsSubmitter` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de junio de 2018 a las 21:12 UTC
- Hora de edición: 10 de junio de 2019 a las 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticTranscoder_ReadOnlyAccess

Descripción: concede a los usuarios acceso de solo lectura a Elastic Transcoder y acceso de lista a los servicios relacionados.

`AmazonElasticTranscoder_ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticTranscoder_ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de junio de 2018 a las 21:09 UTC
- Hora de edición: 10 de junio de 2019 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonElasticTranscoderRole

Descripción: política predeterminada para el rol de servicio de Amazon Elastic Transcoder.

`AmazonElasticTranscoderRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonElasticTranscoderRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 13 de junio de 2019 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRCleanupPolicy

Descripción: Permite las acciones que EMR requiere para terminar y eliminar AWS EC2 recursos si la función del servicio EMR ha perdido esa capacidad.

`AmazonEMRCleanupPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de septiembre de 2017 a las 23:54 UTC
- Hora de edición: 29 de septiembre de 2020 a las 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRContainersServiceRolePolicy

Descripción: Permite el acceso a otros recursos de AWS servicio necesarios para ejecutar Amazon EMR

`AmazonEMRContainersServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de diciembre de 2020 a las 00:38 UTC
- Hora de edición: 6 de febrero de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRFullAccessPolicy_v2

Descripción: proporciona acceso completo a Amazon EMR

`AmazonEMRFullAccessPolicy_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEMRFullAccessPolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de marzo de 2021 a la 1:50 UTC
- Hora editada: 27 de marzo de 2025 a las 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRReadOnlyAccessPolicy_v2

Descripción: Proporciona acceso de solo lectura a Amazon EMR y a las métricas asociadas CloudWatch .

`AmazonEMRReadOnlyAccessPolicy_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEMRReadOnlyAccessPolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 12 de marzo de 2021 a las 1:39 UTC
- Hora de edición: 2 de agosto de 2023 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRServerlessServiceRolePolicy

Descripción: Permite el acceso a otros recursos de AWS servicio necesarios para ejecutar Amazon EMRServerless

`AmazonEMRServerlessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de mayo de 2022 a las 23:15 UTC

- Hora de edición: 25 de enero de 2024 a las 18:21 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEMRServicePolicy_v2

Descripción: esta política es utilizada por el rol de servicio de Amazon EMR y NO se debe utilizar para ningún otro usuario o rol de IAM en la cuenta. La política otorga permisos para crear y administrar los recursos asociados con EMR y los servicios relacionados necesarios para el funcionamiento del clúster de EMR.

`AmazonEMRServicePolicy_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEMRServicePolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de marzo de 2021 a la 1:11 UTC
- Hora editada: 3 de marzo de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonESCognitoAccess

Descripción: proporciona acceso limitado al servicio de configuración de Amazon Cognito.

`AmazonESCognitoAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonESCognitoAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de febrero de 2018 a las 22:29 UTC
- Hora de edición: 20 de diciembre de 2021 a las 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonESFullAccess

Descripción: proporciona acceso completo al servicio de configuración de Amazon ES.

`AmazonESFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonESFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de octubre de 2015 a las 19:14 UTC
- Hora de edición: 1 de octubre de 2015 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonESReadOnlyAccess

Descripción: proporciona acceso de solo lectura al servicio de configuración de Amazon ES.

`AmazonESReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonESReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de octubre de 2015 a las 19:18 UTC
- Hora de edición: 3 de octubre de 2018 a las 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeApiDestinationsServiceRolePolicy

Descripción: Permite acceder EventBridge a los recursos de Secret Manager en su nombre.

`AmazonEventBridgeApiDestinationsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 11 de febrero de 2021 a las 20:52 UTC
- Hora editada: 29 de mayo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeFullAccess

Descripción: Proporciona acceso completo a Amazon EventBridge.

`AmazonEventBridgeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de julio de 2019 a las 14:08 UTC
- Hora editada: 22 de enero de 2025 a las 01:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgePipesFullAccess

Descripción: Proporciona acceso completo a Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgePipesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2022 a las 17:03 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgePipesOperatorAccess

Descripción: Proporciona acceso de solo lectura y de operador (capacidad para detener e iniciar el funcionamiento de tuberías) a Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgePipesOperatorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 1 de diciembre de 2022 a las 17:04 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgePipesReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgePipesReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 1 de diciembre de 2022 a las 17:04 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de julio de 2019 a las 13:59 UTC
- Hora de edición: 1 de diciembre de 2022 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeSchedulerFullAccess

Descripción: La política AmazonEventBridgeSchedulerFullAccess administrada otorga permisos para usar todas las acciones del EventBridge programador para los horarios y grupos de horarios.

`AmazonEventBridgeSchedulerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeSchedulerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de noviembre de 2022 a las 18:37 UTC
- Hora editada: 16 de mayo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeSchedulerReadOnlyAccess

Descripción: La política AmazonEventBridgeSchedulerReadOnlyAccess gestionada concede permisos de solo lectura para ver los detalles sobre sus programaciones y grupos de programaciones

`AmazonEventBridgeSchedulerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeSchedulerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 10 de noviembre de 2022 a las 18:50 UTC
- Hora editada: 16 de mayo de 2025 a las 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeSchemasFullAccess

Descripción: Proporciona acceso completo a Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeSchemasFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2019 a las 23:12 UTC
- Hora de edición: 28 de noviembre de 2019 a las 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeSchemasReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonEventBridgeSchemasReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 28 de noviembre de 2019 a las 23:05 UTC
- Hora de edición: 1 de mayo de 2020 a las 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEventBridgeSchemasServiceRolePolicy

Descripción: Otorga permisos a las reglas gestionadas creadas por los EventBridge esquemas de Amazon.

`AmazonEventBridgeSchemasServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2019 a la 1:10 UTC
- Hora de edición: 27 de noviembre de 2019 a la 1:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonEVSServiceRolePolicy

Descripción: Otorga permisos a EVS para gestionar los recursos en su nombre

`AmazonEVSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de mayo de 2025 a las 23:37 UTC
- Hora editada: 16 de mayo de 2025 a las 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFISServiceRolePolicy

Descripción: Política que permite al AWS FIS gestionar la supervisión y la selección de recursos para los experimentos.

`AmazonFISServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2020 a las 21:18 UTC
- Hora de edición: 25 de octubre de 2022 a las 09:05 UTC

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

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonForecastFullAccess

Descripción: brinda acceso a todas las acciones para Amazon Forecast

`AmazonForecastFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonForecastFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de enero de 2019 a la 1:52 UTC
- Hora de edición: 18 de enero de 2019 a la 1:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFraudDetectorFullAccessPolicy

Descripción: brinda acceso a todas las acciones para Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFraudDetectorFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 22:46 UTC
- Hora de edición: 3 de diciembre de 2019 a las 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFreeRTOSFullAccess

Descripción: política de acceso completo para Amazon FreeRTOS

`AmazonFreeRTOSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFreeRTOSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 15:32 UTC
- Hora de edición: 29 de noviembre de 2017 a las 15:32 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFreeRTOSOTAUpdate

Descripción: permite al usuario acceder a Amazon FreeRTOS OTA Update

`AmazonFreeRTOSOTAUpdate` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFreeRTOSOTAUpdate` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de agosto de 2018 a las 22:43 UTC
- Hora de edición: 18 de diciembre de 2020 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFSxConsoleFullAccess

Descripción: Proporciona acceso completo a Amazon FSx y acceso a los AWS servicios relacionados a través del AWS Management Console.

`AmazonFSxConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFSxConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 16:36 UTC
- Hora editada: 25 de junio de 2025 a las 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Versión de la política

Versión de la política: v13 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFSxConsoleReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon FSx y acceso a AWS servicios relacionados a través del AWS Management Console.

`AmazonFSxConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFSxConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 16:35 UTC
- Hora editada: 25 de febrero de 2025 a las 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFSxFullAccess

Descripción: Proporciona acceso completo a Amazon FSx y acceso a AWS servicios relacionados.

`AmazonFSxFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFSxFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 16:34 UTC
- Hora editada: 25 de junio de 2025 a las 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Versión de la política

Versión de la política: v11 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFSxReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon FSx.

`AmazonFSxReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonFSxReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 16:33 UTC
- Hora de edición: 28 de noviembre de 2018 a las 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonFSxServiceRolePolicy

Descripción: Permite FSx a Amazon gestionar AWS los recursos en tu nombre

`AmazonFSxServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 28 de noviembre de 2018 a las 10:38 UTC
- Hora de edición: 10 de enero de 2024 a las 20:53 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "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-*"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGlacierFullAccess

Descripción: Proporciona acceso completo a Amazon Glacier a través de AWS Management Console.

`AmazonGlacierFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGlacierFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGlacierReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon Glacier a través del AWS Management Console.

`AmazonGlacierReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGlacierReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 5 de mayo de 2016 a las 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGrafanaAthenaAccess

Descripción: esta política concede acceso a Amazon Athena y a las dependencias que se necesitan para permitir la consulta y la escritura de resultados en S3 desde el complemento de Amazon Athena en Amazon Grafana.

`AmazonGrafanaAthenaAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGrafanaAthenaAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de noviembre de 2021 a las 17:11 UTC
- Hora de edición: 22 de noviembre de 2021 a las 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGrafanaCloudWatchAccess

Descripción: Esta política otorga acceso a Amazon CloudWatch y a las dependencias necesarias para su uso CloudWatch como fuente de datos en Amazon Managed Grafana.

`AmazonGrafanaCloudWatchAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGrafanaCloudWatchAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de marzo de 2023 a las 22:41 UTC
- Hora de edición: 24 de marzo de 2023 a las 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGrafanaRedshiftAccess

Descripción: esta política concede acceso delimitado a Amazon Redshift y a las dependencias necesarias para utilizar el complemento de Amazon Redshift en Amazon Grafana.

`AmazonGrafanaRedshiftAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGrafanaRedshiftAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de noviembre de 2021 a las 23:15 UTC
- Hora de edición: 26 de noviembre de 2021 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGrafanaServiceLinkedRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por Amazon Grafana.

`AmazonGrafanaServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de noviembre de 2022 a las 23:10 UTC
- Hora de edición: 8 de noviembre de 2022 a las 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGuardDutyFullAccess

Descripción: Proporciona acceso completo para usar Amazon GuardDuty.

`AmazonGuardDutyFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGuardDutyFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2017 a las 22:31 UTC
- Hora de edición: 10 de junio de 2024 a las 22:50 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "AllowPassRoleToMalwareProtectionPlan",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGuardDutyFullAccess_v2

Descripción: Proporciona acceso completo para usar Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGuardDutyFullAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de junio de 2025 a las 20:22 UTC

- Hora editada: 4 de junio de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "PassRoleToMalwareProtectionPlan",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Descripción: la protección contra el GuardDuty malware utiliza el rol vinculado al servicio (SLR) denominado. AWSService RoleForAmazonGuardDutyMalwareProtection Esta función vinculada al servicio permite a la protección contra GuardDuty malware realizar escaneos sin agentes para detectar malware. Permite GuardDuty crear instantáneas en su cuenta y compartirlas con la cuenta de GuardDuty servicio para detectar malware. Evalúa estas instantáneas compartidas e incluye los metadatos de las EC2 instancias recuperadas en las conclusiones sobre la protección contra el GuardDuty malware. La función AWSService RoleForAmazonGuardDutyMalwareProtection vinculada al servicio confía en que el servicio malware-protection.guardduty.amazonaws.com la asumirá.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de julio de 2022 a las 19:06 UTC
- Hora de edición: 25 de enero de 2024 a las 22:24 h UTC

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

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGuardDutyReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los GuardDuty recursos de Amazon

`AmazonGuardDutyReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonGuardDutyReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2017 a las 22:29 UTC
- Hora de edición: 16 de noviembre de 2023 a las 23:07 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonGuardDutyServiceRolePolicy

Descripción: Habilitar el acceso a AWS los recursos utilizados o administrados por Amazon Guard Duty

`AmazonGuardDutyServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de noviembre de 2017 a las 20:12 UTC
- Hora de edición: 12 de agosto de 2024 a las 20:01 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
```

```
      ],
      "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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHealthLakeFullAccess

Descripción: Proporciona acceso completo al HealthLake servicio de Amazon.

`AmazonHealthLakeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHealthLakeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de febrero de 2021 a la 1:07 UTC
- Hora de edición: 17 de febrero de 2021 a la 1:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHealthLakeReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al HealthLake servicio de Amazon.

`AmazonHealthLakeReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHealthLakeReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de febrero de 2021 a las 2:43 UTC
- Hora de edición: 17 de febrero de 2021 a las 2:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeFullAccess

Descripción: Proporciona acceso completo a Honeycode a través del AWS Management Console SDK.

`AmazonHoneycodeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 24 de junio de 2020 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Honeycode a través del AWS Management Console SDK.

`AmazonHoneycodeReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeServiceRolePolicy

Descripción: un rol vinculado al servicio que se necesita para que Amazon Honeycode acceda a los recursos.

`AmazonHoneycodeServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2020 a las 18:03 UTC
- Hora de edición: 18 de noviembre de 2020 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeTeamAssociationFullAccess

Descripción: Proporciona acceso completo a Honeycode Team Association a través del AWS Management Console SDK.

`AmazonHoneycodeTeamAssociationFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeTeamAssociationFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 24 de junio de 2020 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeTeamAssociationReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Honeycode Team Association a través del AWS Management Console SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeTeamAssociationReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2020 a las 20:27 UTC
- Hora de edición: 24 de junio de 2020 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeWorkbookFullAccess

Descripción: Proporciona acceso completo al Honeycode Workbook a través del SDK AWS Management Console .

`AmazonHoneycodeWorkbookFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeWorkbookFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonHoneycodeWorkbookReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Honeycode Workbook a través del SDK AWS Management Console .

`AmazonHoneycodeWorkbookReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonHoneycodeWorkbookReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 24 de junio de 2020 a las 20:28 UTC
- Hora de edición: 1 de diciembre de 2020 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2AgentlessServiceRolePolicy

Descripción: Concede a Amazon Inspector acceso a las evaluaciones de Servicios de AWS seguridad necesarias para realizar las evaluaciones de seguridad sin agentes

`AmazonInspector2AgentlessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de noviembre de 2023 a las 15:18 h UTC
- Hora de edición: 20 de noviembre de 2023 a las 15:18 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2FullAccess

Descripción: proporciona acceso completo a Amazon Inspector y acceso a otros servicios relacionados, como las organizaciones.

`AmazonInspector2FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspector2FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 19:10 UTC

- Hora de edición: 25 de abril de 2024 a las 13:21 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2FullAccess_v2

Descripción: Proporciona acceso completo a Amazon Inspector y acceso a otros servicios relacionados, como las organizaciones con acceso organizacional restringido.

`AmazonInspector2FullAccess_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspector2FullAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de julio de 2025 a las 16:07 UTC
- Hora editada: 3 de julio de 2025 a las 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:*:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:*:organizations::*:account/o-*/*"
    },
    {
```

```
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2ManagedCisPolicy

Descripción: se trata de una política administrada que el cliente debe asociar a los roles para comunicarse con el servicio de inspección para los análisis CIS

`AmazonInspector2ManagedCisPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspector2ManagedCisPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de enero de 2024 a las 16:31 h UTC
- Hora de edición: 24 de enero de 2024 a las 16:31 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2ReadOnlyAccess

Descripción: proporciona acceso de solo lectura al servicio de Amazon inspector2 y a los servicios de soporte pertinentes

`AmazonInspector2ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspector2ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de enero de 2022 a las 14:45 UTC
- Hora de edición: 22 de septiembre de 2023 a las 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspector2ServiceRolePolicy

Descripción: Otorga a Amazon Inspector acceso a las evaluaciones de seguridad Servicios de AWS necesarias para realizar las evaluaciones de seguridad

`AmazonInspector2ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2021 a las 20:27 UTC
- Hora editada: 29 de abril de 2025 a las 17:37 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Versión de la política

Versión de la política: v16 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "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/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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspectorFullAccess

Descripción: proporciona acceso completo a Amazon Inspector.

`AmazonInspectorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspectorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de octubre de 2015 a las 17:08 UTC
- Hora de edición: 21 de diciembre de 2017 a las 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspectorReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Inspector.

`AmazonInspectorReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonInspectorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de octubre de 2015 a las 17:08 UTC
- Hora de edición: 1 de octubre de 2019 a las 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonInspectorServiceRolePolicy

Descripción: Otorga a Amazon Inspector acceso a las evaluaciones de seguridad Servicios de AWS necesarias para realizar las evaluaciones de seguridad

`AmazonInspectorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de noviembre de 2017 a las 15:48 UTC
- Hora de edición: 11 de septiembre de 2020 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKendraFullAccess

Descripción: Proporciona acceso completo a Amazon Kendra a través de. AWS Management Console

`AmazonKendraFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKendraFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 16:15 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKendraReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon Kendra a través del. AWS Management Console

`AmazonKendraReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKendraReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 16:13 UTC
- Hora de edición: 27 de mayo de 2021 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKeyspacesFullAccess

Descripción: proporciona acceso completo a Amazon Keyspaces

`AmazonKeyspacesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKeyspacesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de abril de 2020 a las 17:06 UTC
- Hora editada: 30 de junio de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKeyspacesReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKeyspacesReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de abril de 2020 a las 17:07 UTC
- Hora editada: 30 de junio de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKeyspacesReadOnlyAccess_v2

Descripción: Proporcione acceso de solo lectura a Amazon Keyspaces y servicios relacionados AWS .

`AmazonKeyspacesReadOnlyAccess_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKeyspacesReadOnlyAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de septiembre de 2023 a las 17:01 UTC
- Hora editada: 27 de junio de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisAnalyticsFullAccess

Descripción: Proporciona acceso completo a Amazon Kinesis Analytics a través del AWS Management Console.

`AmazonKinesisAnalyticsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisAnalyticsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de septiembre de 2016 a las 19:01 UTC
- Hora de edición: 21 de septiembre de 2016 a las 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisAnalyticsReadOnly

Descripción: Proporciona acceso de solo lectura a Amazon Kinesis Analytics a través del. AWS Management Console

`AmazonKinesisAnalyticsReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisAnalyticsReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 21 de septiembre de 2016 a las 18:16 UTC
- Hora de edición: 21 de septiembre de 2016 a las 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisFirehoseFullAccess

Descripción: proporciona acceso completo a todos los flujos de entrega de Amazon Kinesis Firehose.

`AmazonKinesisFirehoseFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisFirehoseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de octubre de 2015 a las 18:45 UTC
- Hora de edición: 7 de octubre de 2015 a las 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisFirehoseReadOnlyAccess

Descripción: proporciona acceso de solo lectura a todos los flujos de entrega de Amazon Kinesis Firehose.

`AmazonKinesisFirehoseReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisFirehoseReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de octubre de 2015 a las 18:43 UTC
- Hora de edición: 7 de octubre de 2015 a las 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisFullAccess

Descripción: Proporciona acceso completo a todas las transmisiones a través del AWS Management Console.

`AmazonKinesisFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a todas las transmisiones a través del AWS Management Console.

`AmazonKinesisReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisVideoStreamsFullAccess

Descripción: Proporciona acceso completo a Amazon Kinesis Video Streams a través del AWS Management Console.

`AmazonKinesisVideoStreamsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisVideoStreamsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2017 a las 23:27 UTC
- Hora de edición: 1 de diciembre de 2017 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonKinesisVideoStreamsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Kinesis Video Streams a través del AWS Management Console.

`AmazonKinesisVideoStreamsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonKinesisVideoStreamsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2017 a las 23:14 UTC

- Hora de edición: 1 de diciembre de 2017 a las 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLaunchWizard_Fullaccess

Descripción: Acceso completo al asistente de AWS lanzamiento y a otros servicios necesarios.

`AmazonLaunchWizard_Fullaccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLaunchWizard_Fullaccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de agosto de 2020 a las 17:47 UTC
- Hora de edición: 22 de febrero de 2023 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLaunchWizardFullAccessV2

Descripción: Acceso completo al asistente de AWS lanzamiento y a otros servicios necesarios.

`AmazonLaunchWizardFullAccessV2` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLaunchWizardFullAccessV2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de septiembre de 2023 a las 17:14 UTC
- Hora de edición: 1 de septiembre de 2023 a las 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexChannelsAccess

Descripción: esta política permite a los clientes llamar al tiempo de ejecución de Lex desde los canales

`AmazonLexChannelsAccess` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2021 a las 20:12 UTC
- Hora de edición: 13 de enero de 2021 a las 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexFullAccess

Descripción: Proporciona acceso completo a Amazon Lex a través de AWS Management Console. También proporciona acceso para crear roles vinculados al Servicio Lex y conceder permisos a Lex para invocar un conjunto limitado de funciones de Lambda.

`AmazonLexFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLexFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de abril de 2017 a las 23:20 UTC
- Hora de edición: 16 de abril de 2024 a las 20:06 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexReadOnly

Descripción: proporciona acceso de solo lectura a Amazon Lex.

`AmazonLexReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLexReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de abril de 2017 a las 23:13 UTC
- Hora de edición: 13 de mayo de 2024 a las 16:58 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexReplicationPolicy

Descripción: permite a Amazon Lex replicar recursos de Lex en las regiones en su nombre.

`AmazonLexReplicationPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 31 de enero de 2024 a las 23:29 h UTC
- Hora editada: 24 de junio de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexRunBotsOnly

Descripción: Proporciona acceso a Amazon Lex conversacional. APIs

`AmazonLexRunBotsOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLexRunBotsOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de abril de 2017 a las 23:06 UTC

- Hora de edición: 18 de agosto de 2021 a las 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLexV2BotPolicy

Descripción: Proporciona a los bots de Lex V2 acceso para llamar a otros AWS servicios en su nombre.

`AmazonLexV2BotPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2021 a las 20:10 UTC
- Hora de edición: 13 de enero de 2021 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutEquipmentFullAccess

Descripción: proporciona acceso completo a las operaciones de Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutEquipmentFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de abril de 2021 a las 15:52 UTC
- Hora de edición: 24 de noviembre de 2021 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutEquipmentReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Lookout for Equipments

`AmazonLookoutEquipmentReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutEquipmentReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 05 de mayo de 2021 a las 16:47 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutMetricsFullAccess

Descripción: proporciona acceso a todas las acciones para Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutMetricsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de mayo de 2021 a las 00:43 UTC
- Hora de edición: 7 de mayo de 2021 a las 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutMetricsReadOnlyAccess

Descripción: proporciona acceso a todas las acciones de solo lectura para Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutMetricsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de mayo de 2021 a las 00:43 UTC
- Hora de edición: 4 de enero de 2022 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutVisionConsoleFullAccess

Descripción: proporciona acceso completo a Amazon Lookout for Vision y acceso delimitado a las dependencias de servicio y consola requeridas.

`AmazonLookoutVisionConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutVisionConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2021 a las 19:37 UTC
- Hora de edición: 11 de mayo de 2021 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutVisionConsoleReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Lookout for Vision y acceso delimitado a las dependencias de servicio y consola requeridas.

`AmazonLookoutVisionConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutVisionConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2021 a las 19:32 UTC
- Hora de edición: 9 de diciembre de 2021 a las 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutVisionFullAccess

Descripción: proporciona acceso completo a Amazon Lookout for Vision y acceso delimitado a las dependencias requeridas.

`AmazonLookoutVisionFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutVisionFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2021 a las 19:24 UTC
- Hora de edición: 11 de mayo de 2021 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonLookoutVisionReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Lookout for Vision y acceso delimitado a las dependencias requeridas.

`AmazonLookoutVisionReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonLookoutVisionReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2021 a las 19:11 UTC
- Hora de edición: 9 de diciembre de 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningBatchPredictionsAccess

Descripción: concede a los usuarios permiso para solicitar predicciones por lotes de Amazon Machine Learning.

`AmazonMachineLearningBatchPredictionsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningBatchPredictionsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:12 UTC
- Hora de edición: 9 de abril de 2015 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningCreateOnlyAccess

Descripción: proporciona acceso de creación a recursos no predictivos de Amazon Machine Learning.

`AmazonMachineLearningCreateOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningCreateOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:18 UTC
- Hora de edición: 29 de junio de 2016 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningFullAccess

Descripción: proporciona acceso completo a los recursos de Amazon Machine Learning.

`AmazonMachineLearningFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:25 UTC
- Hora de edición: 9 de abril de 2015 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Descripción: concede a los usuarios permiso para crear y eliminar el punto de conexión en tiempo real para los modelos de Amazon Machine Learning.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:32 UTC

- Hora de edición: 9 de abril de 2015 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningReadOnlyAccess

Descripción: proporciona acceso de solo lectura a los recursos de Amazon Machine Learning.

`AmazonMachineLearningReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:40 UTC
- Hora de edición: 9 de abril de 2015 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningRealTimePredictionOnlyAccess

Descripción: concede a los usuarios permiso para solicitar predicciones en tiempo real de Amazon Machine Learning.

`AmazonMachineLearningRealTimePredictionOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningRealTimePredictionOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 17:44 UTC
- Hora de edición: 9 de abril de 2015 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMachineLearningRoleforRedshiftDataSourceV3

Descripción: permite que Machine Learning configure y utilice clústeres de Redshift y ubicaciones de preparación de S3 para Redshift Data Source.

`AmazonMachineLearningRoleforRedshiftDataSourceV3` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMachineLearningRoleforRedshiftDataSourceV3` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de junio de 2020 a las 18:00 UTC
- Hora de edición: 24 de junio de 2020 a las 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMacieFullAccess

Descripción: proporciona acceso completo a Amazon Macie.

`AmazonMacieFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMacieFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de agosto de 2017 a las 14:54 UTC
- Hora de edición: 1 de julio de 2022 a las 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMacieHandshakeRole

Descripción: concede permiso para crear el rol vinculado al servicio de Amazon Macie.

`AmazonMacieHandshakeRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMacieHandshakeRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de junio de 2018 a las 15:46 UTC
- Hora de edición: 28 de junio de 2018 a las 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMacieReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Macie.

`AmazonMacieReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMacieReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de junio de 2023 a las 21:50 UTC

- Hora de edición: 15 de junio de 2023 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMacieServiceRole

Descripción: concede a Macie acceso de solo lectura a las dependencias de recursos en la cuenta, para hacer posible el análisis de datos.

`AmazonMacieServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMacieServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 14:53 UTC
- Hora de edición: 14 de agosto de 2017 a las 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMacieServiceRolePolicy

Descripción: rol vinculado al servicio para Amazon Macie

`AmazonMacieServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de junio de 2018 a las 22:17 UTC
- Hora de edición: 19 de mayo de 2022 a las 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonManagedBlockchainConsoleFullAccess

Descripción: Proporciona acceso completo a Amazon Managed Blockchain a través del AWS Management Console

`AmazonManagedBlockchainConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonManagedBlockchainConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de abril de 2019 a las 21:23 UTC
- Hora de edición: 29 de abril de 2019 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonManagedBlockchainFullAccess

Descripción: proporciona acceso completo a Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonManagedBlockchainFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de abril de 2019 a las 21:39 UTC
- Hora de edición: 29 de abril de 2019 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonManagedBlockchainReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonManagedBlockchainReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de abril de 2019 a las 18:17 UTC
- Hora de edición: 30 de abril de 2019 a las 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonManagedBlockchainServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por Amazon Managed Blockchain

`AmazonManagedBlockchainServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de enero de 2020 a las 19:51 UTC
- Hora de edición: 17 de enero de 2020 a las 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMCSFullAccess

Descripción: proporciona acceso completo a Amazon Managed Apache Cassandra Service

`AmazonMCSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMCSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 13:45 UTC
- Hora de edición: 17 de abril de 2020 a las 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMCSReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Managed Apache Cassandra Service

`AmazonMCSReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMCSReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 13:46 UTC
- Hora de edición: 17 de abril de 2020 a las 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMechanicalTurkFullAccess

Descripción: Ofrece acceso completo a todo APIs el contenido de Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMechanicalTurkFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de diciembre de 2015 a las 19:08 UTC
- Hora de edición: 11 de diciembre de 2015 a las 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMechanicalTurkReadOnly

Descripción: proporciona acceso de solo lectura APIs en Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMechanicalTurkReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de diciembre de 2015 a las 19:08 UTC
- Hora de edición: 25 de septiembre de 2019 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMemoryDBFullAccess

Descripción: Proporciona acceso completo a Amazon MemoryDB a través de. AWS Management Console

`AmazonMemoryDBFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMemoryDBFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de octubre de 2021 a las 19:24 UTC

- Hora de edición: 8 de octubre de 2021 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMemoryDBReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon MemoryDB a través de. AWS Management Console

`AmazonMemoryDBReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMemoryDBReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de octubre de 2021 a las 19:27 UTC
- Hora de edición: 8 de octubre de 2021 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMobileAnalyticsFinancialReportAccess

Descripción: proporciona acceso de solo lectura a todos los informes, incluidos los datos financieros, para todos los recursos de la aplicación.

`AmazonMobileAnalyticsFinancialReportAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMobileAnalyticsFinancialReportAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMobileAnalyticsFullAccess

Descripción: proporciona acceso completo a todos los recursos de la aplicación.

`AmazonMobileAnalyticsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMobileAnalyticsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMobileAnalyticsNon-financialReportAccess

Descripción: proporciona acceso de solo lectura a los informes no financieros para todos los recursos de la aplicación.

`AmazonMobileAnalyticsNon-financialReportAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMobileAnalyticsNon-financialReportAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMobileAnalyticsWriteOnlyAccess

Descripción: proporciona acceso de solo escritura para colocar datos de eventos de todos los recursos de la aplicación. (Se recomienda para la integración del SDK)

`AmazonMobileAnalyticsWriteOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMobileAnalyticsWriteOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMonitronFullAccess

Descripción: proporciona acceso completo para administrar Amazon Monitron

`AmazonMonitronFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMonitronFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 2 de diciembre de 2020 a las 22:40 UTC
- Hora de edición: 8 de junio de 2022 a las 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMQApiFullAccess

Descripción: proporciona acceso completo a AmazonMQ a través de nuestra API/SDK.

`AmazonMQApiFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMQApiFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de diciembre de 2018 a las 20:31 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMQApiReadOnlyAccess

Descripción: proporciona acceso de solo lectura a AmazonMQ a través de nuestra API/SDK.

`AmazonMQApiReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMQApiReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de diciembre de 2018 a las 20:31 UTC
- Hora de edición: 18 de diciembre de 2018 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMQFullAccess

Descripción: Proporciona acceso completo a AmazonMQ a través de. AWS Management Console

`AmazonMQFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMQFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 28 de noviembre de 2017 a las 15:28 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMQReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AmazonMQ a través del. AWS Management Console

`AmazonMQReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMQReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 28 de noviembre de 2017 a las 15:30 UTC
- Hora de edición: 28 de noviembre de 2017 a las 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMQServiceRolePolicy

Descripción: Política de funciones vinculadas a servicios para AWS Amazon MQ

`AmazonMQServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de noviembre de 2020 a las 16:07 UTC
- Hora de edición: 4 de noviembre de 2020 a las 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMSKConnectReadOnlyAccess

Descripción: proporcionar acceso de solo lectura a Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMSKConnectReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de septiembre de 2021 a las 10:18 UTC
- Hora de edición: 18 de octubre de 2021 a las 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMSKFullAccess

Descripción: proporciona acceso completo a Amazon MSK y otros permisos necesarios para sus dependencias.

`AmazonMSKFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMSKFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de enero de 2019 a las 22:07 UTC
- Hora de edición: 18 de octubre de 2023 a las 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMSKReadOnlyAccess

Descripción: proporcionar acceso de solo lectura a Amazon MSK

`AmazonMSKReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonMSKReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 14 de enero de 2019 a las 22:28 UTC
- Hora de edición: 14 de enero de 2019 a las 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonMWAAServiceRolePolicy

Descripción: el rol vinculado al servicio utilizado por Amazon Managed Workflows para Apache Airflow.

`AmazonMWAAServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de noviembre de 2020 a las 14:13 UTC
- Hora de edición: 17 de noviembre de 2022 a las 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonNimbleStudio-LaunchProfileWorker

Descripción: esta política concede acceso a los recursos que necesitan los trabajadores de Nimble Studio Launch Profile. Adjunta esta política a las EC2 instancias creadas por Nimble Studio Builder.

`AmazonNimbleStudio-LaunchProfileWorker` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonNimbleStudio-LaunchProfileWorker` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de abril de 2021 a las 4:47 UTC
- Hora de edición: 28 de abril de 2021 a las 4:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonNimbleStudio-StudioAdmin

Descripción: esta política concede acceso a los recursos de Amazon Nimble Studio asociados al administrador del estudio y a los recursos del estudio relacionados en otros servicios. Adjunte esta política al rol de administrador asociado a su estudio.

`AmazonNimbleStudio-StudioAdmin` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonNimbleStudio-StudioAdmin` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de abril de 2021 a las 4:47 UTC
- Hora de edición: 22 de septiembre de 2023 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonNimbleStudio-StudioUser

Descripción: esta política concede acceso a los recursos de Amazon Nimble Studio asociados al usuario del estudio y a los recursos del estudio relacionados en otros servicios. Adjunte esta política al rol de usuario asociado a su estudio.

`AmazonNimbleStudio-StudioUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonNimbleStudio-StudioUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de abril de 2021 a las 4:48 UTC
- Hora de edición: 22 de septiembre de 2023 a las 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonODBServiceRolePolicy

Descripción: Permite a Oracle Database@AWS gestionar AWS los recursos en su nombre.

`AmazonODBServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de noviembre de 2024 a las 18:21 UTC
- Hora editada: 3 de julio de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOmicsFullAccess

Descripción: proporciona acceso completo a Amazon Omics y otros Servicios de AWS necesarios. Esta política permite al usuario ver y aceptar las invitaciones a compartir RAM para acceder a recursos ajenos a los del usuario Cuenta de AWS.

`AmazonOmicsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOmicsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de febrero de 2023 a las 00:59 UTC
- Hora de edición: 24 de febrero de 2023 a las 00:59 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOmicsReadOnlyAccess

Descripción: proporcionar acceso de solo lectura a Amazon Omics

`AmazonOmicsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOmicsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2022 a las 4:17 UTC
- Hora de edición: 29 de noviembre de 2022 a las 4:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOneEnterpriseFullAccess

Descripción: esta política concede permisos administrativos que brindan acceso a todos los recursos y operaciones de Amazon One Enterprise.

`AmazonOneEnterpriseFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOneEnterpriseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2023 a las 04:58 h UTC
- Hora de edición: 28 de noviembre de 2023 a las 04:58 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOneEnterpriseInstallerAccess

Descripción: esta política concede permisos de lectura y escritura limitados que permiten la instalación y activación del dispositivo.

`AmazonOneEnterpriseInstallerAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOneEnterpriseInstallerAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2023 a las 05:00 h UTC
- Hora de edición: 28 de noviembre de 2023 a las 05:00 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOneEnterpriseReadOnlyAccess

Descripción: esta política concede permisos de solo lectura a todos los recursos y operaciones de Amazon One Enterprise.

`AmazonOneEnterpriseReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOneEnterpriseReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2023 a las 04:59 h UTC
- Hora de edición: 28 de noviembre de 2023 a las 04:59 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchDashboardsServiceRolePolicy

Descripción: Proporciona acceso al servicio Amazon OpenSearch Dashboards para acceder a otros AWS servicios, por ejemplo, CloudWatch en su nombre

`AmazonOpenSearchDashboardsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de diciembre de 2023 a las 19:38 h UTC
- Hora de edición: 22 de diciembre de 2023 a las 19:38 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchDirectQueryGlueCreateAccess

Descripción: Permite a OpenSearch DirectQuery Service acceder a AWS Glue APIs para crear recursos en tu nombre.

`AmazonOpenSearchDirectQueryGlueCreateAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchDirectQueryGlueCreateAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 06 de mayo de 2024 a las 12:24 h UTC
- Hora de edición: 06 de mayo de 2024 a las 12:24 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchIngestionFullAccess

Descripción: Permite que Amazon OpenSearch Ingestion acceda a otros AWS servicios en su nombre.

`AmazonOpenSearchIngestionFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchIngestionFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de abril de 2023 a las 18:11 UTC
- Hora de edición: 26 de abril de 2023 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchIngestionReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchIngestionReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de abril de 2023 a las 18:09 UTC
- Hora de edición: 26 de abril de 2023 a las 18:09 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchIngestionServiceRolePolicy

Descripción: Permite que Amazon OpenSearch Ingestion Service acceda a otros AWS servicios en su nombre.

`AmazonOpenSearchIngestionServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2022 a las 16:49 UTC
- Hora de edición: 18 de noviembre de 2022 a las 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchServerlessServiceRolePolicy

Descripción: Permita que Amazon OpenSearch Serverless acceda a otros AWS servicios, por ejemplo, CloudWatch APIs en su nombre.

`AmazonOpenSearchServerlessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de noviembre de 2022 a las 19:50 UTC
- Hora de edición: 25 de julio de 2024 a las 21:19 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchServiceCognitoAccess

Descripción: proporciona acceso al servicio de configuración de Amazon Cognito.

`AmazonOpenSearchServiceCognitoAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchServiceCognitoAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de septiembre de 2021 a las 6:31 UTC
- Hora de edición: 20 de diciembre de 2021 a las 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchServiceFullAccess

Descripción: Proporciona acceso completo al servicio de configuración OpenSearch de Amazon Service.

`AmazonOpenSearchServiceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchServiceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de septiembre de 2021 a las 5:33 UTC
- Hora de edición: 8 de septiembre de 2021 a las 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchServiceReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al servicio de configuración de Amazon OpenSearch Service.

`AmazonOpenSearchServiceReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonOpenSearchServiceReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de septiembre de 2021 a las 5:38 UTC
- Hora de edición: 8 de septiembre de 2021 a las 5:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonOpenSearchServiceRolePolicy

Descripción: Permita que Amazon OpenSearch Service acceda a otros AWS servicios, como las EC2 redes, APIs en su nombre.

`AmazonOpenSearchServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de agosto de 2021 a las 9:27 UTC
- Hora editada: 27 de marzo de 2025 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPersonalizeFullAccess

Descripción: Proporciona acceso completo a Amazon Personalize mediante el SDK AWS Management Console y. También proporciona acceso selecto a servicios relacionados (por ejemplo, S3 CloudWatch).

`AmazonPersonalizeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPersonalizeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de diciembre de 2018 a las 22:24 UTC
- Hora de edición: 30 de mayo de 2019 a las 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPollyFullAccess

Descripción: concede acceso completo a los servicios y recursos de Amazon Polly.

`AmazonPollyFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPollyFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2016 a las 18:59 UTC
- Hora de edición: 30 de noviembre de 2016 a las 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPollyReadOnlyAccess

Descripción: concede acceso de solo lectura a los recursos de Amazon Polly.

`AmazonPollyReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPollyReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2016 a las 18:59 UTC
- Hora de edición: 17 de julio de 2018 a las 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPrometheusConsoleFullAccess

Descripción: Otorga acceso completo a los recursos AWS gestionados de Prometheus en la consola AWS

`AmazonPrometheusConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPrometheusConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de diciembre de 2020 a las 18:11 UTC
- Hora editada: 22 de mayo de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPrometheusFullAccess

Descripción: Otorga acceso completo a los recursos AWS gestionados de Prometheus

`AmazonPrometheusFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPrometheusFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de diciembre de 2020 a las 18:10 UTC
- Hora de edición: 26 de noviembre de 2023 a las 20:16 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPrometheusQueryAccess

Descripción: Otorga acceso para ejecutar consultas en los recursos AWS gestionados de Prometheus

`AmazonPrometheusQueryAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPrometheusQueryAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de diciembre de 2020 a la 1:02 UTC
- Hora de edición: 19 de diciembre de 2020 a la 1:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPrometheusRemoteWriteAccess

Descripción: Otorga acceso de escritura únicamente a los espacios de trabajo AWS gestionados de Prometheus

`AmazonPrometheusRemoteWriteAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonPrometheusRemoteWriteAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de diciembre de 2020 a las 1:04 UTC
- Hora de edición: 19 de diciembre de 2020 a las 1:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonPrometheusScraperServiceRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por Amazon Managed Service for Prometheus Collector

`AmazonPrometheusScraperServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2023 a las 14:19 h UTC
- Hora de edición: 26 de abril de 2024 a las 20:25 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
```

```
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonQDeveloperAccess

Descripción: proporciona acceso de desarrollador para permitir interacciones con Amazon Q

`AmazonQDeveloperAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonQDeveloperAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2024 a las 08:35 h UTC
- Hora editada: 12 de mayo de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonQFullAccess

Descripción: proporciona acceso completo para permitir las interacciones con Amazon Q

`AmazonQFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonQFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2023 a las 16:00 h UTC
- Hora editada: 12 de mayo de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonQLDBConsoleFullAccess

Descripción: Proporciona acceso completo a Amazon QLDB a través del. AWS Management Console

`AmazonQLDBConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonQLDBConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 5 de septiembre de 2019 a las 18:24 UTC
- Hora de edición: 4 de noviembre de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonQLDBFullAccess

Descripción: proporciona acceso completo a Amazon QLDB a través de la API de servicio.

`AmazonQLDBFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonQLDBFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de septiembre de 2019 a las 18:23 UTC

- Hora de edición: 4 de noviembre de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonQLDBReadOnly

Descripción: proporciona acceso de solo lectura a Amazon QLDB.

`AmazonQLDBReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonQLDBReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de septiembre de 2019 a las 18:19 UTC
- Hora de edición: 2 de julio de 2021 a las 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSBetaServiceRolePolicy

Descripción: Permite a Amazon RDS gestionar AWS los recursos en su nombre.

`AmazonRDSBetaServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2018 a las 19:41 UTC
- Hora de edición: 7 de agosto de 2024 a las 00:54 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSCustomInstanceProfileRolePolicy

Descripción: Permite a Amazon RDS Custom realizar diversas acciones de automatización y tareas de administración de bases de datos a través de un perfil de EC2 instancia.

`AmazonRDSCustomInstanceProfileRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSCustomInstanceProfileRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de febrero de 2024 a las 17:42 h UTC
- Hora editada: 20 de marzo de 2025 a las 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSCustomPreviewServiceRolePolicy

Descripción: política de rol de servicio de versión preliminar de Amazon RDS Custom

`AmazonRDSCustomPreviewServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de octubre de 2021 a las 21:44 UTC
- Hora editada: 25 de marzo de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:CopySnapshot",
        "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" : "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSCustomServiceRolePolicy

Descripción: Permite a Amazon RDS Custom gestionar AWS los recursos en su nombre.

`AmazonRDSCustomServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de octubre de 2021 a las 21:39 UTC
- Hora de edición: 25 de marzo de 2025 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:CopySnapshot",
        "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" : "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" : "*"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSDataFullAccess

Descripción: Permite el acceso total para utilizar los datos de RDS APIs, el almacén secreto APIs para las credenciales de la base de datos de RDS y la administración de consultas de la consola de base de datos APIs para ejecutar sentencias SQL en los clústeres de Aurora Serverless del. Cuenta de AWS

`AmazonRDSDataFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSDataFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 20 de noviembre de 2018 a las 21:29 UTC
- Hora de edición: 20 de noviembre de 2019 a las 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSDirectoryServiceAccess

Descripción: permite a RDS acceder a Directory Service Managed AD en nombre del cliente para las instancias de base de datos de SQL Server incorporadas a un dominio.

`AmazonRDSDirectoryServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSDirectoryServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de febrero de 2016 a las 2:02 UTC
- Hora de edición: 15 de mayo de 2019 a las 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSEnhancedMonitoringRole

Descripción: proporciona acceso a CloudWatch para Supervisión mejorada de RDS

`AmazonRDSEnhancedMonitoringRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSEnhancedMonitoringRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de noviembre de 2015 a las 19:58 UTC
- Hora de edición: 11 de noviembre de 2015 a las 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSFullAccess

Descripción: Proporciona acceso completo a Amazon RDS a través de AWS Management Console.

`AmazonRDSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 17 de agosto de 2023 a las 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSPerformanceInsightsFullAccess

Descripción: Proporciona acceso completo a RDS Performance Insights a través del AWS Management Console

`AmazonRDSPerformanceInsightsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSPerformanceInsightsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de agosto de 2023 a las 23:41 UTC
- Hora de edición: 23 de octubre de 2023 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSPerformanceInsightsReadOnly

Descripción: política de solo lectura para Información de rendimiento de RDS

`AmazonRDSPerformanceInsightsReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSPerformanceInsightsReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de abril de 2022 a las 00:02 UTC
- Hora de edición: 23 de octubre de 2023 a las 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "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" : "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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSPreviewServiceRolePolicy

Descripción: política de rol de servicio de versión preliminar de Amazon RDS

`AmazonRDSPreviewServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 31 de mayo de 2018 a las 18:02 UTC
- Hora de edición: 7 de agosto de 2024 a las 01:02 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon RDS a través del AWS Management Console.

`AmazonRDSReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRDSReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 14 de abril de 2023 a las 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRDSServiceRolePolicy

Descripción: Permite a Amazon RDS gestionar AWS los recursos en su nombre.

`AmazonRDSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de enero de 2018 a las 18:17 UTC
- Hora de edición: 01 de julio de 2024 a las 22:42 h UTC

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

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftAllCommandsFullAccess

Descripción: esta política incluye permisos para ejecutar comandos SQL para copiar, cargar, descargar, consultar y analizar datos en Amazon Redshift. La política también otorga permisos para ejecutar determinadas declaraciones para servicios relacionados, como Amazon S3, Amazon CloudWatch logs SageMaker, Amazon o AWS Glue.

`AmazonRedshiftAllCommandsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftAllCommandsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de noviembre de 2021 a las 00:48 UTC
- Hora de edición: 25 de noviembre de 2021 a las 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftDataFullAccess

Descripción: Esta política proporciona acceso total a Amazon Redshift Data. APIs Esta política también concede acceso definido a otros servicios requeridos.

`AmazonRedshiftDataFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftDataFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de septiembre de 2020 a las 19:23 UTC
- Hora de edición: 7 de abril de 2023 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftFullAccess

Descripción: Proporciona acceso completo a Amazon Redshift a través de. AWS Management Console

`AmazonRedshiftFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de julio de 2022 a las 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftQueryEditor

Descripción: proporciona acceso completo al Editor de consultas de Amazon Redshift y a las consultas guardadas a través de la AWS Management Console.

`AmazonRedshiftQueryEditor` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditor` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de octubre de 2018 a las 22:50 UTC
- Hora de edición: 16 de febrero de 2021 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftQueryEditorV2FullAccess

Descripción: concede acceso completo a las operaciones y los recursos del Editor de consultas v2 de Amazon Redshift. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift, leer claves y alias en AWS KMS y administrar los secretos del Query Editor V2 en Secrets Manager AWS .

`AmazonRedshiftQueryEditorV2FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditorV2FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 24 de septiembre de 2021 a las 14:06 UTC
- Hora de edición: 21 de febrero de 2024 a las 17:20 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftQueryEditorV2NoSharing

Descripción: permite trabajar con el Editor de consultas v2 de Amazon Redshift sin compartir recursos. La entidad principal autorizada solo puede leer, actualizar y eliminar sus propios recursos, pero no puede compartirlos. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2NoSharing` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditorV2NoSharing` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 24 de septiembre de 2021 a las 14:18 UTC
- Hora de edición: 21 de febrero de 2024 a las 17:25 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftQueryEditorV2ReadSharing

Descripción: permite trabajar con el Editor de consultas v2 de Amazon Redshift con uso compartido de recursos limitado. La entidad principal concedida puede leer, escribir y compartir sus propios recursos. La entidad principal concedida puede leer los recursos compartidos con su equipo, pero no puede actualizarlos. Esta política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadSharing` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditorV2ReadSharing` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 24 de septiembre de 2021 a las 14:22 UTC
- Hora de edición: 21 de febrero de 2024 a las 17:27 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftQueryEditorV2ReadWriteSharing

Descripción: permite trabajar con el Editor de consultas v2 de Amazon Redshift con uso compartido de recursos. La entidad principal concedida puede leer, escribir y compartir sus propios recursos. La entidad principal concedida puede leer y actualizar los recursos compartidos con su equipo. Esta

política también concede acceso a otros servicios requeridos. Esto incluye permisos para enumerar los clústeres de Amazon Redshift y administrar los secretos del editor de consultas V2 del director en AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadWriteSharing` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftQueryEditorV2ReadWriteSharing` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 24 de septiembre de 2021 a las 14:25 UTC
- Hora de edición: 21 de febrero de 2024 a las 17:30 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon Redshift a través del. AWS Management Console

`AmazonRedshiftReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRedshiftReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 8 de febrero de 2024 a las 00:24 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRedshiftServiceLinkedRolePolicy

Descripción: Permite a Amazon Redshift llamar a los AWS servicios en su nombre

`AmazonRedshiftServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2017 a las 19:19 UTC
- Hora editada: 19 de febrero de 2025 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRekognitionCustomLabelsFullAccess

Descripción: esta política especifica los permisos de Rekognition y S3 que la característica de Etiquetas personalizadas de Amazon Rekognition necesita.

`AmazonRekognitionCustomLabelsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRekognitionCustomLabelsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de enero de 2020 a las 19:18 UTC

- Hora de edición: 16 de agosto de 2022 a las 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRekognitionFullAccess

Descripción: Acceso a todos los Amazon Rekognition APIs

`AmazonRekognitionFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRekognitionFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de noviembre de 2016 a las 14:40 UTC
- Hora de edición: 30 de noviembre de 2016 a las 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRekognitionReadOnlyAccess

Descripción: Acceso a todos los reconocimientos de lectura APIs

`AmazonRekognitionReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRekognitionReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de noviembre de 2016 a las 14:58 UTC
- Hora de edición: 8 de noviembre de 2023 a las 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRekognitionServiceRole

Descripción: Permite que Rekognition llame a AWS los servicios en su nombre.

`AmazonRekognitionServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRekognitionServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de noviembre de 2017 a las 16:52 UTC
- Hora de edición: 29 de noviembre de 2017 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53AutoNamingFullAccess

Descripción: proporciona acceso completo a todas las acciones de denominación automática de Route 53.

`AmazonRoute53AutoNamingFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53AutoNamingFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de enero de 2018 a las 18:40 UTC
- Hora de edición: 18 de enero de 2018 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53AutoNamingReadOnlyAccess

Descripción: proporciona acceso de solo lectura a todas las acciones de denominación automática de Route 53.

`AmazonRoute53AutoNamingReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53AutoNamingReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de enero de 2018 a las 03:02 UTC
- Hora de edición: 18 de enero de 2018 a las 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53AutoNamingRegistrantAccess

Descripción: proporciona acceso a nivel de registrante a las acciones de denominación automática de Route 53.

`AmazonRoute53AutoNamingRegistrantAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53AutoNamingRegistrantAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de marzo de 2018 a las 22:33 UTC
- Hora de edición: 12 de marzo de 2018 a las 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53DomainsFullAccess

Descripción: proporciona acceso completo a todas las acciones de Route53 Domains y Crear zona alojada para permitir la creación de zonas alojadas como parte de los registros de dominio.

`AmazonRoute53DomainsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53DomainsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53DomainsReadOnlyAccess

Descripción: proporciona acceso a la lista y las acciones de Route53 Domains.

`AmazonRoute53DomainsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53DomainsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53FullAccess

Descripción: proporciona acceso completo a Amazon Route 53 a través de la AWS Management Console.

`AmazonRoute53FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 15 de mayo de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53ProfilesFullAccess

Descripción: esta política concede acceso completo a los recursos de Amazon Route 53 Profile.

`AmazonRoute53ProfilesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53ProfilesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de abril de 2024 a las 18:30 h UTC
- Hora de edición: 27 de agosto de 2024 a las 19:18 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53ProfilesReadOnlyAccess

Descripción: esta política concede acceso solo de lectura a los recursos de Amazon Route 53 Profile.

`AmazonRoute53ProfilesReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53ProfilesReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de abril de 2024 a las 18:29 h UTC
- Hora de edición: 27 de agosto de 2024 a las 18:59 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53ReadOnlyAccess

Descripción: proporciona acceso de solo lectura a todo Amazon Route 53 a través de la AWS Management Console.

`AmazonRoute53ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 15 de noviembre de 2016 a las 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryClusterFullAccess

Descripción: proporciona acceso completo al Clúster de recuperación de Amazon Route 53

`AmazonRoute53RecoveryClusterFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryClusterFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de agosto de 2021 a las 18:37 UTC
- Hora de edición: 18 de agosto de 2021 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryClusterReadOnlyAccess

Descripción: proporciona acceso de solo lectura al Clúster de recuperación de Amazon Route 53

`AmazonRoute53RecoveryClusterReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryClusterReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de agosto de 2021 a las 17:36 UTC
- Hora de edición: 1 de abril de 2022 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryControlConfigFullAccess

Descripción: proporciona acceso completo a Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryControlConfigFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 18 de agosto de 2021 a las 17:48 UTC
- Hora de edición: 18 de agosto de 2021 a las 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryControlConfigReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de agosto de 2021 a las 18:01 UTC
- Hora de edición: 18 de octubre de 2023 a las 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryReadinessFullAccess

Descripción: proporciona acceso completo a Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryReadinessFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de agosto de 2021 a las 16:45 UTC

- Hora de edición: 18 de agosto de 2021 a las 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53RecoveryReadinessReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53RecoveryReadinessReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de agosto de 2021 a las 18:11 UTC
- Hora de edición: 9 de noviembre de 2021 a las 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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::*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53ResolverFullAccess

Descripción: política de acceso completo para Route 53 Resolver

`AmazonRoute53ResolverFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53ResolverFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 30 de mayo de 2019 a las 18:10 UTC
- Hora de edición: 05 de agosto de 2024 a las 20:06 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonRoute53ResolverReadOnlyAccess

Descripción: política de solo lectura para Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonRoute53ResolverReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de mayo de 2019 a las 18:11 UTC
- Hora de edición: 05 de agosto de 2024 a las 18:54 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3FullAccess

Descripción: Proporciona acceso completo a todos los depósitos a través del AWS Management Console.

`AmazonS3FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de septiembre de 2021 a las 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3ObjectLambdaExecutionRolePolicy

Descripción: Proporciona permisos a las funciones de AWS Lambda para interactuar con Amazon S3 Object Lambda. También concede permisos a Lambda para escribir en los registros. CloudWatch

`AmazonS3ObjectLambdaExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3ObjectLambdaExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de agosto de 2021 a las 10:07 UTC
- Hora de edición: 18 de agosto de 2021 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3OutpostsFullAccess

Descripción: Proporciona acceso completo a Amazon S3 en Outposts a través del. AWS Management Console

`AmazonS3OutpostsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3OutpostsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de octubre de 2020 a las 17:26 UTC
- Hora de edición: 2 de octubre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3OutpostsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon S3 en Outposts a través del. AWS Management Console

`AmazonS3OutpostsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3OutpostsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de octubre de 2020 a las 18:55 UTC
- Hora de edición: 2 de octubre de 2020 a las 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3ReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a todos los depósitos a través del AWS Management Console.

`AmazonS3ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 10 de agosto de 2023 a las 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3TablesFullAccess

Descripción: Proporciona acceso completo a todos los cubos de tablas de S3.

`AmazonS3TablesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3TablesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:21 UTC
- Hora editada: 3 de diciembre de 2024 a las 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3TablesLakeFormationServiceRole

Descripción: Esta política administrada otorga a AWS Lake Formation permisos para actuar en todos los grupos de tablas, espacios de nombres y tablas de la cuenta.

`AmazonS3TablesLakeFormationServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3TablesLakeFormationServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de junio de 2025 a las 19:07 UTC
- Hora editada: 9 de julio de 2025 a las 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonS3TablesReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a todos los cubos de tablas de S3.

`AmazonS3TablesReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonS3TablesReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:21 UTC
- Hora editada: 3 de diciembre de 2024 a las 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Descripción: Política de funciones de servicio utilizada por el servicio de Servicio de AWS catálogo para aprovisionar productos de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados CodePipeline CodeBuild CodeCommit, incluidos, CloudFormation, Glue, etc.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2020 a las 18:48 UTC
- Hora de edición: 01 de julio de 2024 a las 07:33 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : "arn:aws:codeconnections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasAIServicesAccess

Descripción: Proporciona permisos para que Amazon SageMaker Canvas utilice los servicios de IA a fin de admitir soluciones de IA listas para usar. Esta política añadirá más permisos de mutación para los servicios a medida que Amazon SageMaker Canvas vaya añadiendo compatibilidad.

`AmazonSageMakerCanvasAIServicesAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasAIServicesAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de marzo de 2023 a las 22:36 UTC
- Hora de edición: 29 de noviembre de 2023 a las 14:47 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasBedrockAccess

Descripción: Esta política otorga permisos para usar Amazon Bedrock en SageMaker Canvas al proporcionar acceso a servicios descendentes como S3.

`AmazonSageMakerCanvasBedrockAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasBedrockAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 02 de febrero de 2024 a las 18:37 h UTC
- Hora de edición: 02 de febrero de 2024 a las 18:37 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasDataPrepFullAccess

Descripción: Proporciona acceso completo a SageMaker los recursos y operaciones de Amazon para la preparación de datos en Canvas. La política también proporciona acceso selecto a servicios relacionados (por ejemplo, S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena EventBridge, Glue o Secrets Manager). Esta política debe adjuntarse a la función de ejecución del SageMaker dominio o perfil de usuario de Amazon.

`AmazonSageMakerCanvasDataPrepFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasDataPrepFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de octubre de 2023 a las 22:56 UTC
- Hora de edición: 16 de agosto de 2024 a las 18:11 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasDirectDeployAccess

Descripción: Permite a Amazon SageMaker Canvas crear, gestionar y ver los detalles de los puntos de conexión creados a través de Canvas. Permite a Amazon SageMaker Canvas recuperar las métricas de invocación de puntos finales de CloudWatch.

`AmazonSageMakerCanvasDirectDeployAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasDirectDeployAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de octubre de 2023 a las 18:11 UTC
- Hora de edición: 6 de octubre de 2023 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Descripción: Esta política concede permisos a Amazon EMR Serverless para servicios como S3, que Amazon SageMaker Canvas utiliza para el procesamiento de datos de gran tamaño.

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de julio de 2024 a las 00:35 h UTC
- Hora de edición: 27 de julio de 2024 a las 00:35 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasForecastAccess

Descripción: Esta política concede los permisos que normalmente se necesitan para usar SageMaker Canvas con Amazon Forecast.

`AmazonSageMakerCanvasForecastAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasForecastAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de agosto de 2022 a las 20:04 UTC
- Hora de edición: 24 de agosto de 2022 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasFullAccess

Descripción: Proporciona acceso completo a los recursos y operaciones de Amazon SageMaker Canvas. La política también proporciona acceso selecto a servicios relacionados (por ejemplo, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager y Forecast). Esta política debe adjuntarse a la función de ejecución del SageMaker dominio o perfil de usuario de Amazon.

`AmazonSageMakerCanvasFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 9 de septiembre de 2022 a las 00:44 UTC
- Hora de edición: 16 de agosto de 2024 a las 04:35 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Descripción: Proporciona permisos para que Amazon SageMaker Canvas utilice el servicio SageMaker Data Science Assistant. Actualmente, el Asistente de Ciencia de Datos utiliza Amazon SageMaker y Amazon Q Developer para procesar las solicitudes de los usuarios.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerCanvasSMDataScienceAssistantAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de diciembre de 2024 a las 14:06 UTC
- Hora editada: 13 de enero de 2025 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerClusterInstanceRolePolicy

Descripción: Esta política concede los permisos que normalmente se necesitan para usar Amazon SageMaker Cluster.

`AmazonSageMakerClusterInstanceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerClusterInstanceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2023 a las 15:11 h UTC
- Hora de edición: 29 de noviembre de 2023 a las 15:11 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerCoreServiceRolePolicy

Descripción: Política gestionada para el rol vinculado a servicios de Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2020 a las 21:40 UTC
- Hora de edición: 21 de diciembre de 2020 a las 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerEdgeDeviceFleetPolicy

Descripción: Proporciona los permisos necesarios para que SageMaker Edge cree y administre una flota de dispositivos para el cliente mediante la conexión a la nube predeterminada.

`AmazonSageMakerEdgeDeviceFleetPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerEdgeDeviceFleetPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de diciembre de 2020 a las 16:17 UTC
- Hora de edición: 8 de diciembre de 2020 a las 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerFeatureStoreAccess

Descripción: Proporciona los permisos necesarios para habilitar la tienda offline para un grupo de SageMaker FeatureStore características de Amazon.

`AmazonSageMakerFeatureStoreAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerFeatureStoreAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 16:24 UTC
- Hora de edición: 5 de diciembre de 2022 a las 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerFullAccess

Descripción: Proporciona acceso completo a Amazon SageMaker a través del SDK AWS Management Console y. También proporciona acceso selecto a servicios relacionados (por ejemplo, S3, ECR, CloudWatch Logs).

`AmazonSageMakerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 13:07 UTC
- Hora editada: 4 de diciembre de 2024 a las 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Versión de la política

Versión de la política: v27 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerGeospatialExecutionRole

Descripción: Esta política proporciona acceso a los servicios que normalmente se necesitan para utilizar la tecnología SageMaker geoespacial.

`AmazonSageMakerGeospatialExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerGeospatialExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de noviembre de 2022 a las 10:08 UTC
- Hora de edición: 10 de mayo de 2023 a las 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerGeospatialFullAccess

Descripción: Esta política concede permisos que permiten el acceso total a Amazon SageMaker Geospatial a través del SDK AWS Management Console y.

`AmazonSageMakerGeospatialFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerGeospatialFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de noviembre de 2022 a las 10:06 UTC
- Hora de edición: 30 de noviembre de 2022 a las 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerGroundTruthExecution

Descripción: Proporciona acceso a AWS los servicios necesarios para ejecutar el trabajo SageMaker GroundTruth de etiquetado

`AmazonSageMakerGroundTruthExecution` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerGroundTruthExecution` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2020 a las 19:30 UTC
- Hora de edición: 29 de abril de 2022 a las 20:49 UTC

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

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerHyperPodObservabilityAdminAccess

Descripción: Esta política proporciona los privilegios administrativos necesarios para configurar la SageMaker HyperPod observabilidad. Permite el acceso a los complementos Amazon Managed Prometheus, Amazon Managed Grafana y EKS. La política también incluye un amplio acceso a Grafana HTTP ServiceAccountTokens en todos los espacios de trabajo de Grafana gestionados APIs por Amazon de su cuenta.

`AmazonSageMakerHyperPodObservabilityAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerHyperPodObservabilityAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 10 de julio de 2025 a las 14:37 UTC
- Hora editada: 10 de julio de 2025 a las 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*: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" : "EKSAddonDescribePodIdentityAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribePodIdentityAssociation",
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*"
    },
    {
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerHyperPodServiceRolePolicy

Descripción: Esta política concede permisos a Amazon SageMaker HyperPod para AWS servicios relacionados, como Amazon EKS, Amazon, CloudWatch etc.

`AmazonSageMakerHyperPodServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 06 de septiembre de 2024 a las 17:04 h UTC
- Hora de edición: 06 de septiembre de 2024 a las 17:04 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerMechanicalTurkAccess

Descripción: Proporciona acceso para crear FlowDefinition recursos de Amazon Augmented AI para cualquier equipo de trabajo.

`AmazonSageMakerMechanicalTurkAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerMechanicalTurkAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 16:19 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerModelGovernanceUseAccess

Descripción: Esta política AWS gestionada concede los permisos necesarios para utilizar todas las funciones de Amazon SageMaker Governance. La política también brinda acceso selecto a los servicios relacionados (por ejemplo, S3 o KMS).

`AmazonSageMakerModelGovernanceUseAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerModelGovernanceUseAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2022 a las 08:58 UTC
- Hora de edición: 04 de junio de 2024 a las 21:48 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerModelRegistryFullAccess

Descripción: esta es una nueva política administrada para el Registro de modelos en SageMaker. Esta es una política independiente que se puede asociar al rol de usuario para acceder a las funcionalidades relacionadas con Model Registry en Sagemaker.

`AmazonSageMakerModelRegistryFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerModelRegistryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de abril de 2023 a las 05:20 UTC
- Hora de edición: 06 de junio de 2024 a las 18:48 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerNotebooksServiceRolePolicy

Descripción: Política gestionada para el rol vinculado a servicios para Amazon SageMaker Notebooks

`AmazonSageMakerNotebooksServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de octubre de 2019 a las 20:27 UTC
- Hora editada: 14 de noviembre de 2024 a las 20:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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" : "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerPartnerAppsFullAccess

Descripción: Permite a los usuarios de aplicaciones SageMaker asociadas de Amazon acceder a las aplicaciones, enumerar las aplicaciones disponibles, lanzar aplicaciones web UIs y conectarse a través del SDK de la aplicación.

`AmazonSageMakerPartnerAppsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerPartnerAppsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de enero de 2025 a las 18:37 UTC
- Hora editada: 17 de enero de 2025 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Descripción: Política de funciones de servicio utilizada por los AWS APIGateway productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos Lambda y otros.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:06 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

Descripción: Política de funciones de servicio utilizada por los AWS CloudFormation productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un subconjunto de servicios relacionados, incluidos Lambda APIGateway y otros.

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:06 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Descripción: Política de funciones de servicio utilizada por AWS Lambda en los productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos Secrets Manager y otros.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de agosto de 2023 a las 15:05 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerPipelinesIntegrations

Descripción: Esta política gestionada por Amazon concede los permisos que normalmente se necesitan para su uso con los pasos de Callback y los pasos de Lambda SageMaker en Model Building Pipelines. Se añade al AmazonSageMaker - ExecutionRole que se puede crear al configurar

Studio. SageMaker También, se puede asociar a cualquier otro rol que se vaya a utilizar para crear o ejecutar pipelines.

`AmazonSageMakerPipelinesIntegrations` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerPipelinesIntegrations` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de julio de 2021 a las 16:35 UTC
- Hora de edición: 17 de febrero de 2023 a las 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerQuickSightVPCPolicy

Descripción: SageMaker Unified Studios utilizará esta política para crear recursos relacionados con la VPC para QuickSight

`AmazonSageMakerQuickSightVPCPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerQuickSightVPCPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 3 de junio de 2025 a las 17:37 UTC
- Hora editada: 3 de junio de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerReadOnly

Descripción: Proporciona acceso de solo lectura a Amazon SageMaker a través del SDK AWS Management Console y.

`AmazonSageMakerReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 13:07 UTC
- Hora de edición: 1 de diciembre de 2021 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Descripción: Política de funciones de servicio utilizada por los AWS APIGateway productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos CloudWatch los registros y otros.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2022 a las 04:25 UTC
- Hora de edición: 25 de marzo de 2022 a las 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleF

Descripción: Política de funciones de servicio utilizada por los AWS CloudFormation productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un subconjunto de servicios relacionados, incluidos otros SageMaker .

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2022 a las 04:26 UTC
- Hora de edición: 25 de marzo de 2022 a las 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Descripción: Política de funciones de servicio utilizada por los AWS CodeBuild productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un subconjunto de servicios relacionados CodePipeline, incluidos, CodeBuild entre otros.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de marzo de 2022 a las 04:27 UTC
- Hora de edición: 11 de junio de 2024 a las 18:45 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Descripción: Política de funciones de servicio utilizada por los AWS CodePipeline productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un subconjunto de servicios relacionados CodePipeline, incluidos, CodeBuild entre otros.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:53 UTC
- Hora de edición: 11 de junio de 2024 a las 18:37 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Descripción: Política de roles de servicio utilizada por los AWS CloudWatch eventos dentro de los productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un subconjunto de servicios relacionados, incluidos otros CodePipeline .

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:53 UTC
- Hora de edición: 22 de febrero de 2022 a las 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Descripción: Política de funciones de servicio utilizada por AWS Firehose en los productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos Firehose y otros.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:54 UTC
- Hora de edición: 22 de febrero de 2022 a las 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Descripción: Política de funciones de servicio utilizada por AWS Glue en los productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos Glue, S3 y otros.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de febrero de 2022 a las 09:51 UTC
- Hora de edición: 26 de agosto de 2022 a las 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Descripción: Política de funciones de servicio utilizada por AWS Lambda en los productos AWS ServiceCatalog aprovisionados de la SageMaker cartera de productos de Amazon. Otorga permisos a un conjunto de servicios relacionados, incluidos ECR, S3 y otros.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de abril de 2022 a las 16:34 UTC
- Hora de edición: 11 de junio de 2024 a las 18:57 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSageMakerTrainingPlanCreateAccess

Descripción: Esta política gestionada por Amazon proporciona los permisos necesarios para crear y gestionar planes de SageMaker formación. Permite a los usuarios crear planes de formación y capacidades reservadas, describir los planes de formación existentes y realizar operaciones de búsqueda y publicación de anuncios.

`AmazonSageMakerTrainingPlanCreateAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSageMakerTrainingPlanCreateAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de diciembre de 2024 a las 13:21 UTC
- Hora editada: 4 de diciembre de 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity"
      ],
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AggTagsToTrainingPlanPermissions",
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSecurityLakeAdministrator

Descripción: proporciona acceso completo a Amazon Security Lake y a los servicios relacionados necesarios para administrar Security Lake.

`AmazonSecurityLakeAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSecurityLakeAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de mayo de 2023 a las 22:04 UTC
- Hora de edición: 23 de febrero de 2024 a las 16:01 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSecurityLakeMetastoreManager

Descripción: Política para el administrador de SecurityLake metatiendas de Amazon, lambda, que permite el acceso a cloudwatch, S3, Glue y SQS.

`AmazonSecurityLakeMetastoreManager` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSecurityLakeMetastoreManager` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 23 de enero de 2024 a las 15:26 h UTC
- Hora de edición: 01 de abril de 2024 a las 20:04 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSecurityLakePermissionsBoundary

Descripción: Amazon Security Lake crea roles de IAM para que orígenes personalizados de terceros escriban datos en un lago de datos, y para que los suscriptores de terceros consuman datos de un lago de datos. A su vez, Amazon Security Lake utiliza esta política al crear estos roles para definir el límite de sus permisos.

`AmazonSecurityLakePermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSecurityLakePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2022 a las 14:11 UTC

- Hora de edición: 14 de mayo de 2024 a las 20:39 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSESFullAccess

Descripción: Proporciona acceso completo a Amazon SES a través del AWS Management Console.

`AmazonSESFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSESFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSESReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon SES a través del AWS Management Console.

`AmazonSESReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSESReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 14 de mayo de 2024 a las 12:03 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSESServiceRolePolicy

Descripción: Permite a SES publicar las métricas de monitoreo CloudWatch básicas de Amazon en nombre de sus recursos de SES

`AmazonSESServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de mayo de 2024 a las 16:02 h UTC
- Hora de edición: 21 de mayo de 2024 a las 16:02 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSNSFullAccess

Descripción: Proporciona acceso completo a Amazon SNS a través de. AWS Management Console

`AmazonSNSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSNSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de septiembre de 2024 a las 22:32 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSNSReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon SNS a través del. AWS Management Console

`AmazonSNSReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSNSReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de septiembre de 2024 a las 22:13 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSNSRole

Descripción: política predeterminada para el rol de servicio de Amazon SNS.

`AmazonSNSRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSNSRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSQSFullAccess

Descripción: Proporciona acceso completo a Amazon SQS a través del. AWS Management Console

`AmazonSQSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSQSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSQSReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon SQS a través del. AWS Management Console

`AmazonSQSReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSQSReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 24 de mayo de 2024 a las 18:16 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMAutomationApproverAccess

Descripción: proporciona acceso para ver ejecuciones de automatización y enviar decisiones de aprobación de automatización en espera de aprobación

`AmazonSSMAutomationApproverAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMAutomationApproverAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de agosto de 2017 a las 23:07 UTC
- Hora de edición: 7 de agosto de 2017 a las 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMAutomationRole

Descripción: Proporciona permisos para que el servicio de EC2 automatización ejecute las actividades definidas en los documentos de automatización

`AmazonSSMAutomationRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMAutomationRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de diciembre de 2016 a las 22:09 UTC
- Hora de edición: 24 de julio de 2017 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMDirectoryServiceAccess

Descripción: esta política permite que el agente SSM acceda a Directory Service en nombre del cliente para unirse al dominio de la instancia administrada.

`AmazonSSMDirectoryServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMDirectoryServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de marzo de 2019 a las 17:44 UTC
- Hora de edición: 15 de marzo de 2019 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMFullAccess

Descripción: proporciona acceso completo a Amazon SSM.

`AmazonSSMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de mayo de 2015 a las 17:39 UTC
- Hora de edición: 20 de noviembre de 2019 a las 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMMaintenanceWindowRole

Descripción: Función de servicio que se utilizará en la ventana EC2 de mantenimiento

`AmazonSSMMaintenanceWindowRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMMaintenanceWindowRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2016 a las 15:57 UTC
- Hora de edición: 27 de julio de 2019 a las 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMManagedEC2InstanceDefaultPolicy

Descripción: Esta política habilita la funcionalidad de AWS Systems Manager en EC2 las instancias.

`AmazonSSMManagedEC2InstanceDefaultPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMManagedEC2InstanceDefaultPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de agosto de 2022 a las 20:54 UTC
- Hora de edición: 16 de julio de 2024 a las 18:14 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMManagedInstanceCore

Descripción: La política de Amazon EC2 Role para habilitar las funciones principales del servicio AWS Systems Manager.

`AmazonSSMManagedInstanceCore` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMManagedInstanceCore` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 15 de marzo de 2019 a las 17:22 UTC
- Hora de edición: 23 de mayo de 2019 a las 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMPatchAssociation

Descripción: proporciona acceso a instancias secundarias para la operación de asociación de revisiones.

`AmazonSSMPatchAssociation` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMPatchAssociation` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de mayo de 2020 a las 16:00 UTC
- Hora de edición: 13 de mayo de 2020 a las 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon SSM.

`AmazonSSMReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSSMReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de mayo de 2015 a las 17:44 UTC
- Hora de edición: 29 de mayo de 2015 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSSMServiceRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por Amazon SSM

`AmazonSSMServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de noviembre de 2017 a las 19:20 UTC
- Hora de edición: 15 de noviembre de 2024 a las 14:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonSumerianFullAccess

Descripción: proporciona acceso completo a Amazon Sumerian.

`AmazonSumerianFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonSumerianFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de abril de 2018 a las 20:14 UTC
- Hora de edición: 24 de abril de 2018 a las 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTextractFullAccess

Descripción: Acceso a todos los Amazon Textract APIs

`AmazonTextractFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTextractFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 19:07 UTC
- Hora de edición: 28 de noviembre de 2018 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "textract:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTextractServiceRole

Descripción: Permite a Textract llamar a los AWS servicios en tu nombre.

`AmazonTextractServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTextractServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de noviembre de 2018 a las 19:12 UTC
- Hora de edición: 28 de noviembre de 2018 a las 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamConsoleFullAccess

Descripción: proporciona acceso completo para administrar Amazon Timestream mediante la AWS Management Console. Tenga en cuenta que esta política también otorga permisos para determinadas operaciones de KMS y para las operaciones que administran las consultas guardadas. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

`AmazonTimestreamConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTimestreamConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora editada: 17 de junio de 2025 a las 13:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamFullAccess

Descripción: proporciona acceso completo a Amazon Timestream. Tenga en cuenta que esta política también otorga acceso a determinadas operaciones de KMS. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

`AmazonTimestreamFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTimestreamFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 26 de noviembre de 2021 a las 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamInfluxDBFullAccess

Descripción: proporciona acceso administrativo completo para crear, actualizar, eliminar y enumerar instancias de Amazon Timestream InfluxDB y crear y enumerar grupos de parámetros. Consulte la documentación para obtener información sobre los permisos adicionales necesarios.

`AmazonTimestreamInfluxDBFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTimestreamInfluxDBFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de marzo de 2024 a las 22:53 h UTC
- Hora editada: 17 de abril de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
      ],
      "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Descripción: Proporciona acceso administrativo para gestionar las instancias y los grupos de parámetros de Amazon Timestream InfluxDB, excepto las operaciones del mercado.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 17 de abril de 2025 a las 17:52 UTC
- Hora editada: 17 de abril de 2025 a las 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
      ],
      "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:::*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamInfluxDBServiceRolePolicy

Descripción: proporciona acceso administrativo completo para crear, actualizar, eliminar y enumerar instancias de Amazon Timestream InfluxDB y crear y enumerar grupos de parámetros. Consulte la documentación para obtener información sobre los permisos adicionales necesarios.

`AmazonTimestreamInfluxDBServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de marzo de 2024 a las 18:53 h UTC
- Hora de edición: 14 de marzo de 2024 a las 18:53 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTimestreamReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Timestream. La política también proporciona permiso para cancelar cualquier consulta en curso. Si utiliza una CMK gestionada por el cliente, consulte la documentación para obtener los permisos adicionales necesarios.

`AmazonTimestreamReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTimestreamReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 05 de junio de 2024 a las 19:11 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTranscribeFullAccess

Descripción: proporciona acceso completo a las operaciones de Amazon Transcribe

`AmazonTranscribeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTranscribeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de abril de 2018 a las 16:06 UTC
- Hora de edición: 4 de abril de 2018 a las 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonTranscribeReadOnlyAccess

Descripción: proporciona acceso a la operación de solo lectura para Amazon Transcribe

`AmazonTranscribeReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonTranscribeReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de abril de 2018 a las 16:05 UTC
- Hora de edición: 4 de abril de 2018 a las 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVerifiedPermissionsFullAccess

Descripción: proporciona acceso completo a Permisos verificados

`AmazonVerifiedPermissionsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVerifiedPermissionsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de octubre de 2024 a las 18:19 h UTC
- Hora de edición: 11 de octubre de 2024 a las 18:19 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVerifiedPermissionsReadOnlyAccess

Descripción: proporciona acceso de solo lectura al servicio de Permisos verificados.

`AmazonVerifiedPermissionsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVerifiedPermissionsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de octubre de 2024 a las 18:25 h UTC
- Hora de edición: 11 de octubre de 2024 a las 18:25 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCCrossAccountNetworkInterfaceOperations

Descripción: proporciona acceso para crear interfaces de red y asociarlas a recursos entre cuentas

`AmazonVPCCrossAccountNetworkInterfaceOperations` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCCrossAccountNetworkInterfaceOperations` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 18 de julio de 2017 a las 20:47 UTC
- Hora de edición: 25 de septiembre de 2023 a las 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCFullAccess

Descripción: Proporciona acceso completo a Amazon VPC a través de. AWS Management Console

`AmazonVPCFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora editada: 9 de diciembre de 2024 a las 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Descripción: Proporciona permisos para describir AWS los recursos, ejecutar Network Access Analyzer y crear o eliminar etiquetas en Network Insights Access Scope y Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de junio de 2023 a las 22:56 UTC
- Hora de edición: 15 de mayo de 2024 a las 21:40 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Descripción: Proporciona permisos para describir los AWS recursos, ejecutar Reachability Analyzer y crear o eliminar etiquetas en Network Insights Path y Network Insights Analysis.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCReachabilityAnalyzerFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 14 de junio de 2023 a las 20:12 UTC
- Hora de edición: 15 de mayo de 2024 a las 20:47 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Descripción: esta política está asociada al rol IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Este rol se implementa en las cuentas de los miembros de una organización, cuando la cuenta de administración permite el acceso confiable a Reachability Analyzer. Proporciona permisos para ver los recursos de toda la organización con la consola Reachability Analyzer.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de mayo de 2023 a las 20:38 UTC
- Hora de edición: 1 de mayo de 2023 a las 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonVPCReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon VPC a través de. AWS Management Console

`AmazonVPCReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonVPCReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC

- Hora editada: 9 de diciembre de 2024 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkDocsFullAccess

Descripción: Proporciona acceso completo a Amazon a WorkDocs través del AWS Management Console

`AmazonWorkDocsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkDocsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de abril de 2020 a las 23:05 UTC
- Hora de edición: 16 de abril de 2020 a las 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkDocsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon WorkDocs a través del AWS Management Console

`AmazonWorkDocsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkDocsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de enero de 2020 a las 23:49 UTC
- Hora de edición: 8 de enero de 2020 a las 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkMailEventsServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por Amazon WorkMail Events

`AmazonWorkMailEventsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de abril de 2019 a las 16:52 UTC
- Hora de edición: 16 de abril de 2019 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkMailFullAccess

Descripción: Proporciona acceso completo a Directory Service WorkMail, SES EC2 y acceso de lectura a los metadatos de KMS.

`AmazonWorkMailFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkMailFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 21 de diciembre de 2020 a las 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkMailMessageFlowFullAccess

Descripción: Acceso completo al flujo de WorkMail mensajes APIs

`AmazonWorkMailMessageFlowFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkMailMessageFlowFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de febrero de 2021 a las 11:08 UTC
- Hora de edición: 11 de febrero de 2021 a las 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkMailMessageFlowReadOnlyAccess

Descripción: Acceso de solo lectura a WorkMail los mensajes de la GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkMailMessageFlowReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de enero de 2021 a las 12:40 UTC
- Hora de edición: 28 de enero de 2021 a las 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkMailReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a WorkMail un SES.

`AmazonWorkMailReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkMailReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 25 de julio de 2019 a las 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesAdmin

Descripción: Proporciona acceso a las acciones WorkSpaces administrativas de Amazon mediante el AWS SDK y la CLI.

`AmazonWorkSpacesAdmin` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesAdmin` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de septiembre de 2015 a las 22:21 UTC
- Hora de edición: 27 de junio de 2024 a las 17:16 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesApplicationManagerAdminAccess

Descripción: Proporciona acceso de administrador para empaquetar una aplicación en Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesApplicationManagerAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de abril de 2015 a las 14:03 UTC
- Hora de edición: 09 de abril de 2015 a las 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : "wam:AuthenticatePackager",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkspacesPCAAccess

Descripción: Esta política administrada proporciona acceso administrativo completo a los recursos de CA privada de AWS Certificate Manager Cuenta de AWS para la autenticación basada en certificados.

`AmazonWorkspacesPCAAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkspacesPCAAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de noviembre de 2022 a las 00:25 UTC
- Hora de edición: 8 de noviembre de 2022 a las 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesPoolServiceAccess

Descripción: Esta política proporciona acceso de AWS WorkSpaces servicio a los recursos de cuentas de cliente necesarios para lanzar grupos de Workspaces

`AmazonWorkSpacesPoolServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesPoolServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2024 a las 16:21 h UTC
- Hora de edición: 27 de junio de 2024 a las 16:21 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesSecureBrowserReadOnly

Descripción: Proporciona acceso de solo lectura a Amazon WorkSpaces Secure Browser y sus dependencias a través del SDK y la AWS Management Console CLI.

`AmazonWorkSpacesSecureBrowserReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesSecureBrowserReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 24 de junio de 2024 a las 20:01 h UTC
- Hora de edición: 24 de junio de 2024 a las 20:01 h UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesSelfServiceAccess

Descripción: Proporciona acceso al servicio de WorkSpaces backend de Amazon para realizar acciones de Workspace Self Service

`AmazonWorkSpacesSelfServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesSelfServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2019 a las 19:22 UTC
- Hora de edición: 27 de junio de 2019 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesServiceAccess

Descripción: Proporciona acceso a la cuenta del cliente al AWS WorkSpaces servicio de lanzamiento de un espacio de trabajo.

`AmazonWorkSpacesServiceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesServiceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2019 a las 19:19 UTC
- Hora de edición: 18 de marzo de 2020 a las 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesThinClientFullAccess

Descripción: Proporciona acceso completo a Amazon WorkSpaces Thin Client, así como acceso limitado a los servicios relacionados necesarios

`AmazonWorkSpacesThinClientFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesThinClientFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 09 de agosto de 2024 a las 07:25 h UTC
- Hora editada: 9 de enero de 2025 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por Amazon WorkSpaces Thin Client Monitoring

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de junio de 2025 a las 19:37 UTC
- Hora editada: 13 de junio de 2025 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesThinClientReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon WorkSpaces Thin Client y sus dependencias

`AmazonWorkSpacesThinClientReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesThinClientReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de julio de 2024 a las 08:50 h UTC
- Hora editada: 9 de enero de 2025 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesWebReadOnly

Descripción: Proporciona acceso de solo lectura a Amazon WorkSpaces Web y sus dependencias a través del SDK y la AWS Management Console CLI.

`AmazonWorkSpacesWebReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonWorkSpacesWebReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de noviembre de 2021 a las 14:20 UTC
- Hora de edición: 2 de noviembre de 2022 a las 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonWorkSpacesWebServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por Amazon WorkSpaces Web

`AmazonWorkSpacesWebServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2021 a las 13:15 UTC
- Hora de edición: 15 de diciembre de 2022 a las 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonZocaloFullAccess

Descripción: proporciona acceso completo a Amazon Zocalo.

`AmazonZocaloFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonZocaloFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmazonZocaloReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Zocalo

`AmazonZocaloReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmazonZocaloReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AmplifyBackendDeployFullAccess

Descripción: Proporciona permisos de acceso total a Amplify para implementar los recursos de backend de Amplify (Amazon AWS AppSync Cognito, Amazon S3 y otros servicios relacionados) a través del kit de desarrollo (CDK) Nube de AWS AWS

`AmplifyBackendDeployFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AmplifyBackendDeployFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de octubre de 2023 a las 21:32 UTC
- Hora de edición: 14 de noviembre de 2024 a las 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

APIGatewayServiceRolePolicy

Descripción: Permite a API Gateway gestionar AWS los recursos asociados en nombre del cliente.

`APIGatewayServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 17:23 UTC
- Hora de edición: 12 de julio de 2021 a las 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AppIntegrationsServiceLinkedRolePolicy

Descripción: Permite AppIntegrations gestionar AppFlow los recursos y publicar datos de CloudWatch métricas en su nombre.

`AppIntegrationsServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de septiembre de 2022 a las 19:42 UTC
- Hora de edición: 30 de septiembre de 2022 a las 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ApplicationAutoScalingForAmazonAppStreamAccess

Descripción: Política para habilitar el escalado automático de aplicaciones para Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ApplicationAutoScalingForAmazonAppStreamAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2017 a las 21:39 UTC
- Hora de edición: 6 de febrero de 2017 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o administrados por la función de exportación continua de Application Discovery Service

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de agosto de 2018 a las 20:22 UTC
- Hora de edición: 13 de agosto de 2018 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AppRunnerNetworkingServiceRolePolicy

Descripción: Permite que AWS AppRunner Networking administre AWS los recursos relacionados en su nombre.

`AppRunnerNetworkingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de enero de 2022 a las 21:02 UTC
- Hora de edición: 12 de enero de 2022 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AppRunnerServiceRolePolicy

Descripción: Permite AWS AppRunner gestionar AWS los recursos relacionados en su nombre.

`AppRunnerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de mayo de 2021 a las 19:15 UTC
- Hora de edición: 14 de mayo de 2021 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AppStudioServiceRolePolicy

Descripción: Permite AppStudio gestionar AWS los recursos asociados en su nombre.

`AppStudioServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de julio de 2024 a las 05:01 h UTC
- Hora editada: 13 de marzo de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AuroraDsqlServiceLinkedRolePolicy

Descripción: Política para el rol vinculado a Amazon Aurora DSQL Service

`AuroraDsqlServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2024 a las 15:06 UTC
- Hora editada: 9 de mayo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingConsoleFullAccess

Descripción: Proporciona acceso completo a Auto Scaling a través del AWS Management Console.

`AutoScalingConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AutoScalingConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2017 a las 19:43 UTC
- Hora de edición: 6 de febrero de 2018 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingConsoleReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Auto Scaling a través del. AWS Management Console

`AutoScalingConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AutoScalingConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 12 de enero de 2017 a las 19:48 UTC
- Hora de edición: 12 de enero de 2017 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingFullAccess

Descripción: proporciona acceso completo a Auto Scaling.

`AutoScalingFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AutoScalingFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2017 a las 19:31 UTC
- Hora de edición: 6 de febrero de 2018 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingNotificationAccessRole

Descripción: Política predeterminada para la función de servicio de acceso a las AutoScaling notificaciones.

`AutoScalingNotificationAccessRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AutoScalingNotificationAccessRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Auto Scaling.

`AutoScalingReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AutoScalingReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2017 a las 19:39 UTC
- Hora de edición: 12 de enero de 2017 a las 19:39 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AutoScalingServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o administrados por Auto Scaling

`AutoScalingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de enero de 2018 a las 23:10 UTC
- Hora de edición: 15 de noviembre de 2024 a las 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "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",
        "events:DescribeRule"
      ],
      "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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-Automation-DiagnosisBucketPolicy

Descripción: Proporciona permisos para acceder al depósito S3 de SSM Diagnosis para diagnosticar y solucionar problemas.

`AWS-SSM-Automation-DiagnosisBucketPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-Automation-DiagnosisBucketPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 23:31 UTC
- Hora editada: 15 de noviembre de 2024 a las 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Descripción: Permita diagnosticar problemas con los servicios de SSM mediante la ejecución de las actividades definidas en los documentos de automatización, que se utilizan principalmente para ejecutar los documentos de automatización en una configuración multicuenta y entre regiones, activando automatizaciones secundarias en las cuentas de los miembros.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:01 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*: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}"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Descripción: Proporcione permiso para diagnosticar problemas con los servicios de SSM mediante la ejecución de las actividades definidas en los documentos de automatización, que se utilizan principalmente para ejecutar los documentos de automatización en una configuración de cuenta o región de destino mediante el diagnóstico del estado del servicio de SSM en todos los nodos.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:08 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : [
        "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Descripción: Proporciona permisos para que las cuentas operativas diagnostiquen los nodos no gestionados, ya que proporciona los permisos específicos de la organización que requiere la automatización de SSM para obtener la lista de cuentas de los miembros de la raíz de una organización y activar la ejecución entre cuentas y regiones, lo que permite asumir funciones de ejecución en la cuenta o región de destino.

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:11 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Descripción: Conceda permiso para solucionar problemas relacionados con los servicios de SSM mediante la ejecución de las actividades definidas en los documentos de automatización, que se utilizan principalmente para ejecutar los documentos de automatización en una configuración multicuenta y entre regiones, activando automatizaciones secundarias en las cuentas de los miembros.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:14 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*: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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Descripción: Proporciona permisos para solucionar problemas relacionados con los servicios de SSM mediante la ejecución de las actividades definidas en los documentos de automatización, que se utilizan principalmente para ejecutar los documentos de automatización en una configuración de cuenta o región de destino mediante la corrección del estado de los servicios de SSM en todos los nodos.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:17 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*: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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Descripción: Proporciona permisos a las cuentas operativas para corregir los nodos no gestionados, ya que proporciona los permisos específicos de la organización que requiere la automatización de SSM para obtener la lista de cuentas de los miembros de la raíz de una organización y activar la ejecución entre cuentas y regiones, lo que permite asumir funciones de ejecución en la cuenta o región de destino.

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` a los usuarios, grupos y roles.

Información de la política

- AWS Tipo: política gestionada
- Hora de creación: 16 de noviembre de 2024 a las 00:25 UTC
- Hora editada: 16 de noviembre de 2024 a las 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWS_ConfigRole

Descripción: Política predeterminada para el rol de servicio AWS Config. Proporciona los permisos necesarios para que AWS Config realice un seguimiento de los cambios en sus AWS recursos.

`AWS_ConfigRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWS_ConfigRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 15 de septiembre de 2020 a las 20:30 UTC
- Hora de edición: 20 de junio de 2025 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Versión de la política

Versión de la política: v38 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
```

```
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "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:GetEventIntegration",
        "app-integrations:ListApplications",
        "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",
        "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:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
```

```
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "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:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock: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:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
```

```
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "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:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
```

```
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "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:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
```

```
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "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",
        "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:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
```

```
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "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:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "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:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "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: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:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "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:ListExperimentTemplates",
        "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: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:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
```

```
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "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:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "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:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "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:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
```

```
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "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",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "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:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "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:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "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:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "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:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "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",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
```

```
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "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:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "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:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:ListChannels",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "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",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "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:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "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:GetDirectoryRegistration",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
```

```
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "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:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
```

```
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "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",
        "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:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver: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:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "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:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
```

```
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
```

```
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "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:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
```

```
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "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:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
```

```
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetServiceSetting",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "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",
        "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:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListServiceNetworks",
        "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:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAccountActivityAccess

Descripción: permite a los usuarios acceder a la página de Actividad de la cuenta.

`AWSAccountActivityAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAccountActivityAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 7 de marzo de 2023 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAccountManagementFullAccess

Descripción: Proporciona acceso completo a la administración de AWS cuentas.

`AWSAccountManagementFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAccountManagementFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de septiembre de 2021 a las 23:20 UTC
- Hora de edición: 30 de septiembre de 2021 a las 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAccountManagementReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la administración de AWS cuentas

`AWSAccountManagementReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAccountManagementReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de septiembre de 2021 a las 23:29 UTC
- Hora de edición: 30 de septiembre de 2021 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAccountUsageReportAccess

Descripción: permite a los usuarios acceder a la página de Informe de uso de la cuenta.

`AWSAccountUsageReportAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAccountUsageReportAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAgentlessDiscoveryService

Descripción: Proporciona acceso al Discovery Agentless Connector para registrarse en AWS Application Discovery Service.

`AWSAgentlessDiscoveryService` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAgentlessDiscoveryService` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 2 de agosto de 2016 a las 01:35 UTC
- Hora de edición: 24 de febrero de 2020 a las 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppFabricFullAccess

Descripción: Proporciona acceso completo al AWS AppFabric servicio y acceso de solo lectura a los servicios dependientes, como S3, Kinesis o KMS.

`AWSAppFabricFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppFabricFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2023 a las 19:51 UTC
- Hora de edición: 27 de junio de 2023 a las 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppFabricReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS AppFabric

`AWSAppFabricReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppFabricReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2023 a las 19:52 UTC
- Hora de edición: 27 de junio de 2023 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppFabricServiceRolePolicy

Descripción: Proporciona AppFabric acceso a AWS los recursos en su nombre

`AWSAppFabricServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2023 a las 21:07 UTC
- Hora de edición: 26 de junio de 2023 a las 21:07 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingAppStreamFleetPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder AppStream y CloudWatch.

`AWSApplicationAutoscalingAppStreamFleetPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 19:04 UTC
- Hora de edición: 20 de octubre de 2017 a las 19:04 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingCassandraTablePolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Cassandra y CloudWatch.

`AWSApplicationAutoscalingCassandraTablePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de marzo de 2020 a las 22:49 UTC
- Hora de edición: 18 de marzo de 2020 a las 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingComprehendEndpointPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Comprehend y. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 14 de noviembre de 2019 a las 18:39 UTC
- Hora de edición: 14 de noviembre de 2019 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoScalingCustomResourcePolicy

Descripción: Política que otorga permisos a Application Auto Scaling CloudWatch para acceder APIGateway y escalar recursos personalizados

`AWSApplicationAutoScalingCustomResourcePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de junio de 2018 a las 23:22 UTC
- Hora de edición: 4 de junio de 2018 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingDynamoDBTablePolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a DynamoDB y. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2017 a las 21:34 UTC
- Hora de edición: 20 de octubre de 2017 a las 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a EC2 Spot Fleet y CloudWatch.

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de octubre de 2017 a las 18:23 UTC
- Hora de edición: 25 de octubre de 2017 a las 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingECSServicePolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a EC2 Container Service y CloudWatch.

`AWSApplicationAutoscalingECSServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de octubre de 2017 a las 23:53 UTC
- Hora de edición: 24 de octubre de 2024 a las 20:05 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingElastiCacheRGPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Amazon ElastiCache y Amazon CloudWatch.

`AWSApplicationAutoscalingElastiCacheRGPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de agosto de 2021 a las 23:41 UTC
- Hora de edición: 26 de marzo de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Elastic Map Reduce y CloudWatch.

`AWSApplicationAutoscalingEMRInstanceGroupPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de octubre de 2017 a las 00:57 UTC
- Hora de edición: 26 de octubre de 2017 a las 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingKafkaClusterPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Managed Streaming for Apache Kafka Kafka y. CloudWatch

`AWSApplicationAutoscalingKafkaClusterPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2020 a las 18:36 UTC
- Hora de edición: 24 de agosto de 2020 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Lambda y. CloudWatch

`AWSApplicationAutoscalingLambdaConcurrencyPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de octubre de 2019 a las 20:04 UTC

- Hora de edición: 21 de octubre de 2019 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingNeptuneClusterPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Amazon Neptune y Amazon. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de septiembre de 2021 a las 21:14 UTC
- Hora de edición: 2 de septiembre de 2021 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingRDSClusterPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a RDS y CloudWatch.

`AWSApplicationAutoscalingRDSClusterPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de octubre de 2017 a las 17:46 UTC
- Hora de edición: 7 de agosto de 2018 a las 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingSageMakerEndpointPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder SageMaker y CloudWatch.

`AWSApplicationAutoscalingSageMakerEndpointPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de febrero de 2018 a las 19:58 UTC
- Hora de edición: 13 de noviembre de 2023 a las 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Descripción: Política que otorga permisos a Application Auto Scaling para acceder a Amazon WorkSpaces y Amazon CloudWatch.

`AWSApplicationAutoscalingWorkSpacesPoolPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de junio de 2024 a las 18:39 h UTC
- Hora de edición: 17 de junio de 2024 a las 18:39 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationDiscoveryAgentAccess

Descripción: Proporciona acceso al Discovery Agent para registrarse en AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationDiscoveryAgentAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2016 a las 21:38 UTC
- Hora de edición: 24 de febrero de 2020 a las 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationDiscoveryAgentlessCollectorAccess

Descripción: permite que los Application Discovery Service Agentless Collectors se actualicen, registren y comuniquen automáticamente con Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationDiscoveryAgentlessCollectorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de agosto de 2022 a las 21:00 UTC
- Hora de edición: 16 de agosto de 2022 a las 21:00 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationDiscoveryServiceFullAccess

Descripción: Proporciona acceso completo para ver y etiquetar los elementos de configuración mantenidos por AWS Application Discovery Service

`AWSApplicationDiscoveryServiceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationDiscoveryServiceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2016 a las 21:30 UTC
- Hora de edición: 19 de junio de 2019 a las 21:21 UTC

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

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationAgentInstallationPolicy

Descripción: Esta política permite instalar el agente de AWS replicación, que se utiliza con el Servicio de migración de AWS aplicaciones (MGN) para migrar AWS servidores externos. Adjunte esta

política a los usuarios o roles de IAM cuyas credenciales proporcione al instalar el agente de AWS replicación.

`AWSApplicationMigrationAgentInstallationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationAgentInstallationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 19 de junio de 2022 a las 07:51 UTC
- Hora de edición: 20 de septiembre de 2022 a las 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationAgentPolicy

Descripción: Esta política permite instalar y usar el agente de AWS replicación, que se usa con el Servicio de migración de AWS aplicaciones (MGN) para migrar AWS servidores externos. Adjunte esta política a los usuarios o roles de IAM cuyas credenciales proporcione al instalar el agente de AWS replicación.

`AWSApplicationMigrationAgentPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationAgentPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS administrada
- Hora de creación: 7 de abril de 2021 a las 07:00 UTC
- Hora de edición: 20 de septiembre de 2022 a las 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationAgentPolicy_v2

Descripción: Esta política permite utilizar el agente de AWS replicación, que se utiliza con el Servicio de migración de AWS aplicaciones (MGN) para migrar servidores externos a AWS ellos. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationAgentPolicy_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationAgentPolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de junio de 2022 a las 14:14 UTC
- Hora de edición: 6 de junio de 2022 a las 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationConversionServerPolicy

Descripción: Esta política permite que el servidor de conversión del Servicio de migración de aplicaciones (MGN), que son EC2 instancias lanzadas por el Servicio de migración de aplicaciones, se comunique con el servicio MGN. MGN asigna una función de IAM con esta política (como perfil de EC2 instancia) a los servidores de conversión de MGN, que MGN lanza y termina automáticamente cuando es necesario. No es recomendable que asocie esta política a sus usuarios o roles de IAM. El Servicio de migración de aplicaciones utiliza los Servidores de conversión MGN cuando los usuarios eligen lanzar instancias de prueba o transición con la consola, la CLI o la API de MGN.

`AWSApplicationMigrationConversionServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationConversionServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 06:48 UTC
- Hora de edición: 7 de abril de 2021 a las 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationEC2Access

Descripción: Esta política proporciona EC2 las operaciones de Amazon necesarias para utilizar el Servicio de migración de aplicaciones (MGN) para lanzar los servidores migrados como EC2 instancias. Asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationEC2Access` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationEC2Access` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de abril de 2021 a las 07:05 UTC
- Hora editada: 11 de febrero de 2025 a las 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationFullAccess

Descripción: Esta política proporciona permisos a todos los públicos APIs del Servicio de Migración de AWS Aplicaciones (MGN), así como permisos para leer la información clave del KMS. Asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de abril de 2021 a las 06:56 UTC
- Hora editada: 2 de julio de 2025 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Versión de la política

Versión de la política: v9 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationMGHAccess

Descripción: Esta política permite a AWS Application Migration Service (MGN) enviar metadatos sobre el progreso de los servidores que se migran mediante MGN a Migration Hub AWS (MGH). MGN crea automáticamente un rol de IAM con esta política asocia y lo adopta. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationMGHAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationMGHAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 07:10 UTC
- Hora de edición: 7 de abril de 2021 a las 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationReadOnlyAccess

Descripción: Esta política proporciona permisos a todos los servicios públicos APIs de solo lectura del Servicio de Migración de Aplicaciones (MGN), así como a algunos otros AWS servicios APIs de solo lectura que son necesarios para poder utilizar la consola de MGN en modo de solo lectura. Asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: AWS política gestionada

- Hora de creación: 7 de abril de 2021 a las 07:15 UTC
- Hora de edición: 20 de marzo de 2023 a las 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationReplicationServerPolicy

Descripción: Esta política permite a los servidores de replicación del Servicio de migración de aplicaciones (MGN), que son EC2 instancias lanzadas por el Servicio de migración de aplicaciones, comunicarse con el servicio MGN y crear instantáneas de EBS en sus servidores. Cuenta de AWS El Servicio de Migración de Aplicaciones asigna una función de IAM con esta política (como perfil de EC2 instancia) a los servidores de replicación de MGN, que MGN inicia y termina automáticamente, según sea necesario. Los servidores de replicación MGN se utilizan para facilitar la replicación de datos desde sus servidores externos AWS, como parte del proceso de migración gestionado mediante MGN. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationReplicationServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationReplicationServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de abril de 2021 a las 07:21 UTC
- Hora de edición: 7 de abril de 2021 a las 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationServiceEc2InstancePolicy

Descripción: Esta política permite instalar y usar el agente de AWS replicación, que utiliza el Servicio de migración de AWS aplicaciones (AWS MGN) para migrar los servidores de origen que se ejecutan en ellos EC2 (entre regiones o entre zonas de disponibilidad). Se debe adjuntar a las instancias una función de IAM con esta política (como perfil de EC2 instancia). EC2

`AWSApplicationMigrationServiceEc2InstancePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationServiceEc2InstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de agosto de 2023 a las 13:19 UTC
- Hora de edición: 3 de enero de 2024 a las 14:19 h UTC

- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationServiceRolePolicy

Descripción: Permite que el Servicio de Migración de AWS Aplicaciones cree y gestione AWS recursos en su nombre.

`AWSApplicationMigrationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 7 de abril de 2021 a las 06:43 UTC
- Hora editada: 16 de marzo de 2025 a las 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationSSMAccess

Descripción: esta política proporciona acceso a las operaciones de Amazon SSM necesarias para utilizar Application Migration Service (MGN) para ejecutar documentos SSM de comandos personalizados tras la migración. Asocie esta política a sus usuarios o roles de IAM.

`AWSApplicationMigrationSSMAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationSSMAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 09:29 UTC
- Hora editada: 2 de julio de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSApplicationMigrationVCenterClientPolicy

Descripción: Esta política permite instalar y utilizar el AWS VCenter cliente, que se utiliza con el Servicio de migración de AWS aplicaciones (MGN) para migrar AWS servidores externos. Adjunte esta política a los usuarios o roles de IAM cuyas credenciales proporcione al instalar el AWS VCenter cliente.

`AWSApplicationMigrationVCenterClientPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSApplicationMigrationVCenterClientPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de noviembre de 2021 a las 12:53 UTC
- Hora de edición: 8 de noviembre de 2021 a las 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshEnvoyAccess

Descripción: política de App Mesh Envoy para obtener acceso a la configuración del nodo virtual.

`AWSAppMeshEnvoyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppMeshEnvoyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de julio de 2019 a las 21:29 UTC
- Hora de edición: 3 de julio de 2019 a las 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshFullAccess

Descripción: Proporciona acceso completo a AWS App Mesh APIs y a la consola de administración.

`AWSAppMeshFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppMeshFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de abril de 2019 a las 17:50 UTC

- Hora de edición: 7 de enero de 2021 a las 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshPreviewEnvoyAccess

Descripción: política de App Mesh Preview Envoy para obtener acceso a la configuración del nodo virtual.

`AWSAppMeshPreviewEnvoyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppMeshPreviewEnvoyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de agosto de 2019 a las 23:32 UTC
- Hora de edición: 5 de agosto de 2019 a las 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshPreviewServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por AWS App Mesh

`AWSAppMeshPreviewServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de junio de 2019 a las 19:07 UTC
- Hora de edición: 21 de agosto de 2019 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshReadOnly

Descripción: Proporciona acceso de solo lectura a AWS App Mesh APIs y a la consola de administración.

`AWSAppMeshReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppMeshReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 16 de abril de 2019 a las 17:51 UTC
- Hora de edición: 7 de enero de 2021 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppMeshServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o gestionados por AWS AppMesh

`AWSAppMeshServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de junio de 2019 a las 18:30 UTC
- Hora de edición: 10 de octubre de 2023 a las 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
```

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppRunnerFullAccess

Descripción: concede permisos a todas las acciones de App Runner.

`AWSAppRunnerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppRunnerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de enero de 2022 a las 04:02 UTC
- Hora de edición: 11 de enero de 2022 a las 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppRunnerReadOnlyAccess

Descripción: concede permisos para enumerar y ver detalles sobre los recursos de App Runner.

`AWSAppRunnerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppRunnerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de febrero de 2022 a las 21:24 UTC
- Hora de edición: 24 de febrero de 2022 a las 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppRunnerServicePolicyForECRAccess

Descripción: Política de servicio de AWS App Runner que otorga permisos de lectura a los recursos de Amazon ECR en la cuenta del cliente. Úsela en un rol que se transfiere a App Runner al crear o actualizar un servicio de App Runner.

`AWSAppRunnerServicePolicyForECRAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppRunnerServicePolicyForECRAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de mayo de 2021 a las 19:17 UTC
- Hora de edición: 14 de mayo de 2021 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppSyncAdministrator

Descripción: Proporciona acceso administrativo al AppSync servicio, aunque no lo suficiente como para acceder a través de la consola.

`AWSAppSyncAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppSyncAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de marzo de 2018 a las 21:20 UTC
- Hora de edición: 4 de noviembre de 2019 a las 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppSyncInvokeFullAccess

Descripción: Proporciona un acceso de invocación completo al AppSync servicio, tanto a través de la consola como de forma independiente

`AWSAppSyncInvokeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppSyncInvokeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de marzo de 2018 a las 21:21 UTC
- Hora de edición: 20 de marzo de 2018 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppSyncPushToCloudWatchLogs

Descripción: Permite AppSync enviar registros a la CloudWatch cuenta del usuario.

`AWSAppSyncPushToCloudWatchLogs` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppSyncPushToCloudWatchLogs` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2018 a las 19:38 UTC
- Hora de edición: 09 de abril de 2018 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppSyncSchemaAuthor

Descripción: proporciona acceso para crear, actualizar y consultar el esquema.

`AWSAppSyncSchemaAuthor` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAppSyncSchemaAuthor` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de marzo de 2018 a las 21:21 UTC
- Hora de edición: 1 de febrero de 2023 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAppSyncServiceRolePolicy

Descripción: Permite el acceso a AWS los servicios y recursos utilizados o administrados por AppSync

`AWSAppSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de enero de 2020 a las 19:56 UTC
- Hora de edición: 21 de enero de 2020 a las 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSArtifactAccountSync

Descripción: Permite el acceso de solo lectura de AWS Artifact a las operaciones de Organizations. AWS

`AWSArtifactAccountSync` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSArtifactAccountSync` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de abril de 2018 a las 23:04 UTC
- Hora de edición: 10 de abril de 2018 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSArtifactAgreementsFullAccess

Descripción: Esta política otorga permisos completos para publicar, descargar, aceptar y rescindir los acuerdos de AWS Artifact. También incluye permisos para enumerar y habilitar el acceso a los AWS servicios en el servicio de la Organización, además de describir los detalles de la organización. Además, la política permite comprobar si existe el rol vinculado al servicio requerido y crea uno si no existe

`AWSArtifactAgreementsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSArtifactAgreementsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de noviembre de 2024 a las 19:36 UTC
- Hora editada: 22 de noviembre de 2024 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSArtifactAgreementsReadOnlyAccess

Descripción: Esta política otorga acceso de solo lectura para enumerar los acuerdos de servicio de AWS Artifact y descargar los acuerdos aceptados. También incluye permisos para enumerar y describir los detalles de la organización. Además, la política permite comprobar si existe el rol vinculado al servicio requerido.

`AWSArtifactAgreementsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSArtifactAgreementsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de noviembre de 2024 a las 19:36 UTC
- Hora editada: 22 de noviembre de 2024 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSArtifactReportsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los informes del servicio AWS Artifact.

`AWSArtifactReportsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSArtifactReportsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 02 de enero de 2024 a las 22:42 h UTC
- Hora editada: 24 de marzo de 2025 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSArtifactServiceRolePolicy

Descripción: Permite a AWS Artifact recopilar información sobre una organización a través del servicio AWS Organizations.

`AWSArtifactServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de agosto de 2023 a las 20:27 UTC
- Hora de edición: 21 de agosto de 2023 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAuditManagerAdministratorAccess

Descripción: Proporciona acceso administrativo para activar o desactivar AWS Audit Manager, actualizar la configuración y gestionar las evaluaciones, los controles y los marcos

`AWSAuditManagerAdministratorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSAuditManagerAdministratorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de diciembre de 2020 a las 20:02 UTC
- Hora de edición: 15 de mayo de 2024 a las 23:46 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAuditManagerServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por AWS Audit Manager

`AWSAuditManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 8 de diciembre de 2020 a las 15:12 UTC
- Hora de edición: 24 de septiembre de 2024 a las 23:22 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "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"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSAutoScalingPlansEC2AutoScalingPolicy

Descripción: Política que otorga permisos a AWS Auto Scaling para pronosticar periódicamente la capacidad y generar acciones de escalado programadas para los grupos de Auto Scaling en un plan de escalado

`AWSAutoScalingPlansEC2AutoScalingPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de agosto de 2018 a las 22:46 UTC
- Hora de edición: 23 de agosto de 2018 a las 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupAuditAccess

Descripción: Esta política otorga permisos a los usuarios para crear controles y marcos que definan sus expectativas con respecto a los recursos y las actividades de AWS Backup, y para auditar los recursos y las actividades de AWS Backup comparándolos con los controles y marcos definidos. Esta política otorga permisos a AWS Config y a servicios similares para describir las expectativas de los usuarios y realizar las auditorías. Esta política también otorga permisos para entregar informes de auditoría a S3 y servicios similares, y permite que los usuarios busquen y abran sus informes de auditoría.

`AWSBackupAuditAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupAuditAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de agosto de 2021 a las 01:02 UTC
- Hora de edición: 10 de abril de 2023 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:::*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupDataTransferAccess

Descripción: Esta política permite al agente AWS Backint completar la transferencia de datos de respaldo con el plano AWS Backup Storage. Adjunte esta política a las funciones que asumen las EC2 instancias que ejecutan SAP HANA con el agente Backint.

`AWSBackupDataTransferAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupDataTransferAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de noviembre de 2022 a las 22:48 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupFullAccess

Descripción: Esta política está destinada a los administradores de copias de seguridad y les otorga acceso total a las operaciones de AWS copia de seguridad, incluida la creación o edición de planes de copia de seguridad, la asignación de AWS recursos a los planes de copia de seguridad, la eliminación de copias de seguridad y la restauración de copias de seguridad.

`AWSBackupFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de noviembre de 2019 a las 22:21 UTC
- Hora editada: 22 de mayo de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Versión de la política

Versión de la política: v20 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Descripción: Proporciona AWS BackupGateway permiso para sincronizar los metadatos de las máquinas virtuales en su nombre

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 15 de diciembre de 2022 a las 19:43 UTC
- Hora de edición: 15 de diciembre de 2022 a las 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupOperatorAccess

Descripción: Esta política otorga a los usuarios permisos para asignar AWS recursos a los planes de respaldo, crear copias de seguridad a pedido y restaurarlas. Esta política no permite que el usuario cree o edite planes de copia de seguridad o elimine copias de seguridad programadas una vez que están creadas.

`AWSBackupOperatorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupOperatorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de noviembre de 2019 a las 22:23 UTC
- Hora editada: 22 de mayo de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Versión de la política

Versión de la política: v18 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupOrganizationAdminAccess

Descripción: esta política está diseñada para los administradores de copias de seguridad que utilizan la administración de copias de seguridad entre cuentas para administrar las copias de seguridad de la organización.

`AWSBackupOrganizationAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupOrganizationAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2020 a las 16:23 UTC
- Hora de edición: 18 de noviembre de 2022 a las 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupRestoreAccessForSAPHANA

Descripción: Proporciona permiso AWS de Backup para restaurar una copia de seguridad de SAP HANA en Amazon EC2

`AWSBackupRestoreAccessForSAPHANA` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupRestoreAccessForSAPHANA` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de noviembre de 2022 a las 22:43 UTC
- Hora de edición: 10 de noviembre de 2022 a las 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupSearchOperatorAccess

Descripción: El rol de operador de búsqueda tiene acceso a crear índices de respaldo y a crear búsquedas de los metadatos de respaldo que se han indexado. Esta política contiene los permisos necesarios para estas funciones de operador de búsqueda.

`AWSBackupSearchOperatorAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupSearchOperatorAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de febrero de 2025 a las 21:52 UTC
- Hora editada: 25 de marzo de 2025 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceLinkedRolePolicyForBackup

Descripción: Proporciona permiso AWS de Backup para crear copias de seguridad en su nombre en todos AWS los servicios

`AWSBackupServiceLinkedRolePolicyForBackup` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de junio de 2020 a las 23:08 UTC
- Hora editada: 22 de mayo de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Versión de la política

Versión de la política: v19 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceLinkedRolePolicyForBackupTest

Descripción: Proporciona permiso AWS de Backup para crear copias de seguridad en su nombre en todos AWS los servicios

`AWSBackupServiceLinkedRolePolicyForBackupTest` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de mayo de 2020 a las 17:37 UTC
- Hora de edición: 12 de mayo de 2020 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForBackup

Descripción: Proporciona permiso AWS de Backup para crear copias de seguridad en su nombre en todos AWS los servicios

`AWSBackupServiceRolePolicyForBackup` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForBackup` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de enero de 2019 a las 21:01 UTC
- Hora editada: 22 de mayo de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Versión de la política

Versión de la política: v22 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForIndexing

Descripción: Política que contiene los permisos necesarios para que AWS Backup indexe los puntos de recuperación.

`AWSBackupServiceRolePolicyForIndexing` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForIndexing` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de diciembre de 2024 a las 18:37 UTC
- Hora editada: 17 de diciembre de 2024 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForItemRestores

Descripción: Política que contiene los permisos necesarios para que AWS Backup restaure elementos individuales en un punto de recuperación

`AWSBackupServiceRolePolicyForItemRestores` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForItemRestores` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de diciembre de 2024 a las 18:37 UTC
- Hora editada: 17 de diciembre de 2024 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForRestores

Descripción: Proporciona permiso AWS de Backup para realizar restauraciones en su nombre en todos AWS los servicios. Esta política incluye permisos para crear y eliminar AWS recursos, como volúmenes de EBS, instancias de RDS y sistemas de archivos EFS, que forman parte del proceso de restauración.

`AWSBackupServiceRolePolicyForRestores` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForRestores` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de enero de 2019 a las 00:23 UTC
- Hora editada: 22 de mayo de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Versión de la política

Versión de la política: v23 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForS3Backup

Descripción: Política que contiene los permisos necesarios para que AWS Backup haga copias de seguridad de los datos en cualquier bucket de S3. Esto incluye el acceso de lectura a todos los objetos de S3 y cualquier acceso de descifrado a todas las claves de KMS.

`AWSBackupServiceRolePolicyForS3Backup` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForS3Backup` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de febrero de 2022 a las 17:40 UTC
- Hora de edición: 17 de mayo de 2024 a las 17:12 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBackupServiceRolePolicyForS3Restore

Descripción: Política que contiene los permisos necesarios para que AWS Backup restaure una copia de seguridad de S3 en un bucket. Esto incluye los permisos de lectura y escritura para todos los buckets de S3 y los permisos DescribeKey para GenerateDataKey y para todas las claves de KMS.

`AWSBackupServiceRolePolicyForS3Restore` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBackupServiceRolePolicyForS3Restore` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 18 de febrero de 2022 a las 17:39 UTC
- Hora de edición: 7 de febrero de 2023 a las 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBatchFullAccess

Descripción: Proporciona acceso completo a los recursos de AWS Batch.

`AWSBatchFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBatchFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de diciembre de 2016 a las 19:35 UTC
- Hora de edición: 24 de octubre de 2022 a las 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBatchServiceEventTargetRole

Descripción: Política para habilitar CloudWatch Event Target para el envío de trabajos AWS por lotes

`AWSBatchServiceEventTargetRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBatchServiceEventTargetRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de febrero de 2018 a las 22:31 UTC
- Hora de edición: 28 de febrero de 2018 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBatchServiceRole

Descripción: Política para la función de servicio AWS Batch que permite el acceso a servicios relacionados EC2, como el escalado automático, el servicio de EC2 contenedores y Cloudwatch Logs.

`AWSBatchServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBatchServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de diciembre de 2016 a las 19:36 UTC
- Hora de edición: 05 de diciembre de 2023 a las 18:49 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Versión de la política

Versión de la política: v13 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBCMDataExportsServiceRolePolicy

Descripción: Función vinculada a un servicio para proporcionar a los exportadores de datos de Billing and Cost Management acceso a los datos del AWS servicio para exportarlos a una ubicación de destino, como Amazon S3, en nombre de un cliente.

`AWSBCMDataExportsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de junio de 2024 a las 17:40 h UTC
- Hora de edición: 10 de junio de 2024 a las 17:40 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBillingConductorFullAccess

Descripción: Utilice la política AWSBilling ConductorFullAccess administrada para permitir el acceso completo a la consola AWS Billing Conductor (ABC) y APIs. Esta política permite a los usuarios enumerar, crear y eliminar los recursos de ABC.

`AWSBillingConductorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBillingConductorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de abril de 2022 a las 18:02 UTC
- Hora de edición: 13 de abril de 2022 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBillingConductorReadOnlyAccess

Descripción: Utilice la política AWSBilling ConductorReadOnlyAccess administrada para permitir el acceso de solo lectura a la consola AWS Billing Conductor (ABC) y APIs. Esta política concede

el permiso para obtener y enumerar todos los recursos de IAM. No incluye la capacidad de crear o eliminar recursos.

`AWSBillingConductorReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBillingConductorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de abril de 2022 a las 18:02 UTC
- Hora de edición: 13 de abril de 2022 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBillingReadOnlyAccess

Descripción: permite a los usuarios ver las facturas en la Consola de facturación.

`AWSBillingReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBillingReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de agosto de 2020 a las 20:08 UTC
- Hora editada: 12 de marzo de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
```

```
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Descripción: Esta política otorga permisos para controlar AWS los recursos. Por ejemplo, para iniciar y detener EC2 instancias de RDS mediante la ejecución de scripts de AWS Systems Manager (SSM).

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 25 de mayo de 2022 a las 19:03 UTC
- Hora de edición: 25 de mayo de 2022 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*: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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBudgetsActionsWithAWSResourceControlAccess

Descripción: Proporciona acceso completo a las acciones de AWS Presupuestos, incluido el uso de las acciones de Presupuestos para controlar el estado de los AWS recursos en funcionamiento mediante AWS Management Console

`AWSBudgetsActionsWithAWSResourceControlAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBudgetsActionsWithAWSResourceControlAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de octubre de 2020 a las 17:19 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBudgetsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la consola de AWS presupuestos a través de AWS Management Console.

`AWSBudgetsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBudgetsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de octubre de 2020 a las 17:18 UTC
- Hora de edición: 17 de junio de 2024 a las 17:41 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBugBustFullAccess

Descripción: Esta política de IAM concede a los usuarios acceso total a la consola AWS BugBust

`AWSBugBustFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBugBustFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2021 a las 07:03 UTC
- Hora de edición: 22 de julio de 2021 a las 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBugBustPlayerAccess

Descripción: Esta política de IAM otorga a los usuarios acceso para participar en eventos AWS BugBust

`AWSBugBustPlayerAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSBugBustPlayerAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2021 a las 07:15 UTC
- Hora de edición: 24 de junio de 2021 a las 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSBugBustServiceRolePolicy

Descripción: Otorga permisos AWS BugBust para acceder a los recursos en su nombre

`AWSBugBustServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de junio de 2021 a las 06:59 UTC
- Hora de edición: 24 de junio de 2021 a las 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerFullAccess

Descripción: Proporciona acceso completo a AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de enero de 2016 a las 17:02 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerPrivateCAAuditor

Descripción: Proporciona acceso de auditor a AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAAuditor` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAAuditor` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de octubre de 2018 a las 16:51 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerPrivateCAFullAccess

Descripción: Proporciona acceso completo a la autoridad de AWS certificación privada de Certificate Manager

`AWSCertificateManagerPrivateCAFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de octubre de 2018 a las 16:54 UTC
- Hora de edición: 23 de octubre de 2018 a las 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerPrivateCAPrivilegedUser

Descripción: Proporciona acceso de usuarios de certificados privilegiados a AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAPrivilegedUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAPrivilegedUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de junio de 2019 a las 17:43 UTC
- Hora editada: 22 de enero de 2025 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerPrivateCAReadOnly

Descripción: Proporciona acceso de solo lectura a AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de octubre de 2018 a las 16:57 UTC
- Hora de edición: 17 de agosto de 2020 a las 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerPrivateCAUser

Descripción: Proporciona acceso de usuario certificado a la AWS entidad de certificación privada de Certificate Manager

`AWSCertificateManagerPrivateCAUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerPrivateCAUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de octubre de 2018 a las 16:53 UTC
- Hora editada: 22 de enero de 2025 a las 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCertificateManagerReadOnly

Descripción: Proporciona acceso de solo lectura a AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCertificateManagerReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de enero de 2016 a las 17:07 UTC
- Hora de edición: 15 de marzo de 2021 a las 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSChatbotServiceLinkedRolePolicy

Descripción: El rol vinculado al servicio que utiliza el AWS Chatbot.

`AWSChatbotServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2019 a las 16:39 UTC
- Hora de edición: 18 de noviembre de 2019 a las 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCleanRoomsFullAccess

Descripción: Permite el acceso total a los recursos de las salas AWS limpias y el acceso a los relacionados Servicios de AWS.

`AWSCleanRoomsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCleanRoomsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2023 a las 16:10 UTC
- Hora de edición: 21 de marzo de 2024 a las 15:35 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCleanRoomsFullAccessNoQuerying

Descripción: Permite el acceso total a los recursos de las salas AWS limpias, excepto para realizar consultas en una colaboración y acceder a los relacionados Servicios de AWS.

`AWSCleanRoomsFullAccessNoQuerying` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCleanRoomsFullAccessNoQuerying` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de enero de 2023 a las 16:12 UTC
- Hora de edición: 14 de mayo de 2024 a las 18:31 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCleanRoomsMLFullAccess

Descripción: Permite el acceso completo a los recursos de aprendizaje automático de AWS Clean Rooms y el acceso a los relacionados Servicios de AWS.

`AWSCleanRoomsMLFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCleanRoomsMLFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2023 a las 21:02 h UTC
- Hora editada: 10 de enero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCleanRoomsMLReadOnlyAccess

Descripción: Permite el acceso de solo lectura a los recursos de aprendizaje automático de salas AWS limpias y el acceso de solo lectura a los recursos de salas limpias relacionados AWS

`AWSCleanRoomsMLReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCleanRoomsMLReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2023 a las 20:55 h UTC
- Hora editada: 10 de enero de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCleanRoomsReadOnlyAccess

Descripción: Permite el acceso de solo lectura a los recursos de AWS Clean Rooms y el acceso de solo lectura a los recursos relacionados de Glue AWS y Amazon Logs. CloudWatch

`AWSCleanRoomsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCleanRoomsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 12 de enero de 2023 a las 16:10 UTC
- Hora de edición: 12 de enero de 2023 a las 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloud9Administrator

Descripción: Proporciona acceso de administrador a AWS Cloud9.

`AWSCloud9Administrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloud9Administrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:17 UTC
- Hora de edición: 11 de octubre de 2023 a las 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloud9EnvironmentMember

Descripción: Ofrece la posibilidad de ser invitado a los entornos de desarrollo compartidos de AWS Cloud9.

`AWSCloud9EnvironmentMember` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloud9EnvironmentMember` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:18 UTC
- Hora editada: 27 de enero de 2025 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloud9ServiceRolePolicy

Descripción: Política de funciones vinculadas a servicios para AWS Cloud9

`AWSCloud9ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2017 a las 13:44 UTC
- Hora de edición: 17 de enero de 2022 a las 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloud9SSMInstanceProfile

Descripción: Esta política se utilizará para asignar un rol a una InstanceProfile que permitirá a Cloud9 usar el administrador de sesiones SSM para conectarse a la instancia

`AWSCloud9SSMInstanceProfile` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloud9SSMInstanceProfile` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 14 de mayo de 2020 a las 11:40 UTC
- Hora de edición: 14 de mayo de 2020 a las 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloud9User

Descripción: Proporciona permiso para crear entornos de desarrollo de AWS Cloud9 y administrar los entornos propios.

`AWSCloud9User` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloud9User` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2017 a las 16:16 UTC
- Hora editada: 27 de enero de 2025 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudFormationFullAccess

Descripción: Proporciona acceso completo a AWS CloudFormation.

`AWSCloudFormationFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudFormationFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de julio de 2019 a las 21:50 UTC
- Hora de edición: 26 de julio de 2019 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudFormationReadOnlyAccess

Descripción: Proporciona acceso a AWS CloudFormation través de AWS Management Console.

`AWSCloudFormationReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudFormationReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 13 de noviembre de 2019 a las 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudFrontLogger

Descripción: Otorga a CloudFront Logger permisos de escritura en los CloudWatch registros.

`AWSCloudFrontLogger` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2018 a las 20:15 UTC
- Hora de edición: 22 de noviembre de 2019 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudFrontVPCOriginServiceRolePolicy

Descripción: Permite administrar CloudFront las interfaces de EC2 Elastic Network y los grupos de seguridad en su nombre.

`AWSCloudFrontVPCOriginServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de octubre de 2024 a las 17:45 h UTC
- Hora de edición: 24 de octubre de 2024 a las 17:45 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudHSMFullAccess

Descripción: proporciona acceso completo a todos los recursos de CloudHSM.

`AWSCloudHSMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudHSMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudHSMReadOnlyAccess

Descripción: proporciona acceso de solo lectura a todos los recursos de CloudHSM.

`AWSCloudHSMReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudHSMReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudHSMRole

Descripción: Política predeterminada para el rol de AWS servicio CloudHSM.

`AWSCloudHSMRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudHSMRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudMapDiscoverInstanceAccess

Descripción: Proporciona acceso a la API de descubrimiento de Nube de AWS mapas.

`AWSCloudMapDiscoverInstanceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudMapDiscoverInstanceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2018 a las 00:02 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudMapFullAccess

Descripción: Proporciona acceso completo a todas las acciones del Nube de AWS mapa.

`AWSCloudMapFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudMapFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 23:57 UTC
- Hora de edición: 29 de julio de 2020 a las 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudMapReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a todas las acciones del Nube de AWS mapa.

`AWSCloudMapReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudMapReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 28 de noviembre de 2018 a las 23:45 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudMapRegisterInstanceAccess

Descripción: Proporciona acceso a nivel de registrante a las acciones del Nube de AWS mapa.

`AWSCloudMapRegisterInstanceAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudMapRegisterInstanceAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2018 a las 00:04 UTC
- Hora de edición: 20 de septiembre de 2023 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudShellFullAccess

Descripción: Las subvenciones se utilizan AWS CloudShell con todas las funciones

`AWSCloudShellFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudShellFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 18:07 UTC

- Hora de edición: 15 de diciembre de 2020 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudTrail_FullAccess

Descripción: Proporciona acceso completo a AWS CloudTrail.

`AWSCloudTrail_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudTrail_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de octubre de 2020 a las 23:41 UTC
- Hora de edición: 22 de febrero de 2021 a las 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudTrail_ReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCloudTrail_ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de junio de 2022 a las 17:19 UTC
- Hora de edición: 14 de junio de 2022 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Descripción: Esta política la utiliza el rol vinculado al servicio denominado. AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents CloudWatch utiliza esta función vinculada al servicio para realizar las acciones del administrador de incidentes AWS del administrador del sistema cuando una CloudWatch alarma pasa al estado de ALARMA. Esta política otorga permiso para iniciar incidentes en su nombre.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de abril de 2021 a las 13:30 UTC
- Hora de edición: 27 de abril de 2021 a las 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeArtifactAdminAccess

Descripción: Proporciona acceso completo a AWS CodeArtifact través de AWS Management Console.

`AWSCodeArtifactAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeArtifactAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de junio de 2020 a las 23:53 UTC
- Hora de edición: 16 de junio de 2020 a las 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeArtifactReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS CodeArtifact través de AWS Management Console.

`AWSCodeArtifactReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeArtifactReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de junio de 2020 a las 21:23 UTC
- Hora de edición: 25 de junio de 2020 a las 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeBuildAdminAccess

Descripción: Proporciona acceso completo a AWS CodeBuild través de AWS Management Console. Adjunte también AmazonS3 ReadOnlyAccess para proporcionar acceso a la descarga de artefactos de construcción y adjunte IAMFull Access para crear y administrar la función de servicio. CodeBuild

`AWSCodeBuildAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeBuildAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 19:04 UTC
- Hora editada: 16 de diciembre de 2024 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeBuildDeveloperAccess

Descripción: Proporciona acceso a AWS CodeBuild través de la administración del CodeBuild proyecto AWS Management Console, pero no la permite. Adjunte también AmazonS3 ReadOnlyAccess para permitir el acceso a la descarga de artefactos de construcción.

`AWSCodeBuildDeveloperAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeBuildDeveloperAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 19:02 UTC
- Hora editada: 16 de diciembre de 2024 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Versión de la política

Versión de la política: v16 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeBuildReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS CodeBuild través de AWS Management Console. Adjunte también AmazonS3 ReadOnlyAccess para proporcionar acceso a la descarga de artefactos de construcción.

`AWSCodeBuildReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeBuildReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 19:03 UTC
- Hora editada: 16 de diciembre de 2024 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Versión de la política

Versión de la política: v13 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeCommitFullAccess

Descripción: Proporciona acceso completo a AWS CodeCommit través de AWS Management Console.

`AWSCodeCommitFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeCommitFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:02 UTC
- Hora editada: 10 de enero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeCommitPowerUser

Descripción: Proporciona acceso completo a AWS CodeCommit los repositorios, pero no permite eliminarlos.

`AWSCodeCommitPowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeCommitPowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:06 UTC
- Hora editada: 10 de enero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Versión de la política

Versión de la política: v16 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeCommitReadOnly

Descripción: Proporciona acceso de solo lectura a AWS CodeCommit través de AWS Management Console.

`AWSCodeCommitReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeCommitReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:05 UTC
- Hora editada: 10 de enero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployDeployerAccess

Descripción: proporciona acceso para registrar e implementar una revisión.

`AWSCodeDeployDeployerAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployDeployerAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de mayo de 2015 a las 18:18 UTC
- Hora editada: 16 de diciembre de 2024 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployFullAccess

Descripción: Proporciona acceso completo a CodeDeploy los recursos.

`AWSCodeDeployFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 19 de mayo de 2015 a las 18:13 UTC
- Hora editada: 16 de diciembre de 2024 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployReadOnlyAccess

Descripción: proporciona acceso de solo lectura a CodeDeploy los recursos.

`AWSCodeDeployReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de mayo de 2015 a las 18:21 UTC
- Hora editada: 16 de diciembre de 2024 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRole

Descripción: Proporciona acceso al CodeDeploy servicio para expandir las etiquetas e interactuar con Auto Scaling en su nombre.

`AWSCodeDeployRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de mayo de 2015 a las 18:05 UTC
- Hora de edición: 16 de agosto de 2023 a las 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRoleForCloudFormation

Descripción: Proporciona acceso al CodeDeploy servicio para invocar la función Lambda en su nombre y realizar una implementación azul/verde de forma automática. CloudFormation

`AWSCodeDeployRoleForCloudFormation` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRoleForCloudFormation` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de mayo de 2020 a las 17:12 UTC
- Hora de edición: 19 de mayo de 2020 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRoleForECS

Descripción: Proporciona acceso a todo el CodeDeploy servicio para realizar una implementación azul/verde de ECS en su nombre. Otorga acceso total a los servicios de soporte, como el acceso total para leer todos los objetos de S3, invocar todas las funciones de Lambda, publicar en todos los temas de SNS de la cuenta y actualizar todos los servicios de ECS.

`AWSCodeDeployRoleForECS` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRoleForECS` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de noviembre de 2018 a las 20:40 UTC
- Hora de edición: 23 de septiembre de 2019 a las 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRoleForECSLimited

Descripción: Proporciona acceso limitado al CodeDeploy servicio para realizar una implementación azul/verde de ECS en su nombre.

`AWSCodeDeployRoleForECSLimited` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRoleForECSLimited` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 27 de noviembre de 2018 a las 20:42 UTC
- Hora de edición: 23 de septiembre de 2019 a las 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRoleForLambda

Descripción: Proporciona acceso al CodeDeploy servicio para realizar una implementación de Lambda en su nombre.

`AWSCodeDeployRoleForLambda` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRoleForLambda` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de noviembre de 2017 a las 14:05 UTC
- Hora de edición: 3 de diciembre de 2019 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeDeployRoleForLambdaLimited

Descripción: Proporciona acceso limitado al CodeDeploy servicio para realizar una implementación de Lambda en su nombre.

`AWSCodeDeployRoleForLambdaLimited` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeDeployRoleForLambdaLimited` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de agosto de 2020 a las 17:14 UTC
- Hora de edición: 17 de agosto de 2020 a las 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodePipeline_FullAccess

Descripción: Proporciona acceso completo a AWS CodePipeline través de AWS Management Console.

`AWSCodePipeline_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodePipeline_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de agosto de 2020 a las 22:38 UTC
- Hora de edición: 14 de marzo de 2024 a las 17:06 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodePipeline_ReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS CodePipeline través de AWS Management Console.

`AWSCodePipeline_ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodePipeline_ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de agosto de 2020 a las 22:25 UTC
- Hora de edición: 3 de agosto de 2020 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodePipelineApproverAccess

Descripción: proporciona acceso para ver y aprobar los cambios manuales para todas las canalizaciones

`AWSCodePipelineApproverAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodePipelineApproverAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de julio de 2016 a las 18:59 UTC
- Hora de edición: 2 de agosto de 2017 a las 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodePipelineCustomActionAccess

Descripción: Proporciona acceso a acciones personalizadas para sondear los detalles de los trabajos (incluidas las credenciales temporales) e informar sobre las actualizaciones de estado AWS CodePipeline.

`AWSCodePipelineCustomActionAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodePipelineCustomActionAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:02 UTC

- Hora de edición: 9 de julio de 2015 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeStarFullAccess

Descripción: Proporciona acceso completo a AWS CodeStar través de AWS Management Console.

`AWSCodeStarFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeStarFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de abril de 2017 a las 16:23 UTC
- Hora de edición: 28 de marzo de 2023 a las 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeStarNotificationsServiceRolePolicy

Descripción: Permite que AWS CodeStar Notifications acceda a Amazon CloudWatch Events en tu nombre

`AWSCodeStarNotificationsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de noviembre de 2019 a las 16:10 UTC
- Hora de edición: 19 de marzo de 2020 a las 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCodeStarServiceRole

Descripción: NO UTILIZAR: Política de funciones de AWS CodeStar servicio que otorga privilegios administrativos CodeStar para gestionar la IAM y otros recursos de servicio en nombre del cliente.

`AWSCodeStarServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCodeStarServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de abril de 2017 a las 15:20 UTC
- Hora de edición: 20 de septiembre de 2021 a las 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCompromisedKeyQuarantine

Descripción: deniega el acceso a determinadas acciones, que el AWS equipo aplica en caso de que las credenciales de un usuario de IAM se vean comprometidas o estén expuestas públicamente. NO elimine esta política. En su lugar, siga las instrucciones especificadas en el correo electrónico que se le envió sobre este evento.

`AWSCompromisedKeyQuarantine` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCompromisedKeyQuarantine` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de agosto de 2020 a las 18:04 UTC
- Hora de edición: 11 de agosto de 2020 a las 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCompromisedKeyQuarantineV2

Descripción: deniega el acceso a determinadas acciones, que el AWS equipo aplica en caso de que las credenciales de un usuario de IAM se vean comprometidas o estén expuestas públicamente. NO elimine esta política. En su lugar, siga las instrucciones especificadas en el caso de soporte que se le creó sobre este evento.

`AWSCompromisedKeyQuarantineV2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCompromisedKeyQuarantineV2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de abril de 2021 a las 22:30 UTC
- Hora de edición: 02 de octubre de 2024 a las 16:41 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCompromisedKeyQuarantineV3

Descripción: deniega el acceso a determinadas acciones y se aplica AWS en caso de que las credenciales de un usuario de IAM se hayan visto comprometidas o estén expuestas públicamente. El objetivo de esta política es limitar los posibles daños causados por actividades fraudulentas que

den lugar a cargos no autorizados, sin que los recursos existentes se vean afectados. NO elimine esta política. En su lugar, siga las instrucciones especificadas en el caso de soporte que se le creó sobre este evento.

`AWSCompromisedKeyQuarantineV3` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCompromisedKeyQuarantineV3` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de agosto de 2024 a las 17:36 h UTC
- Hora de edición: 02 de octubre de 2024 a las 16:52 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigMultiAccountSetupPolicy

Descripción: Permite a Config llamar a AWS servicios e implementar recursos de configuración en toda la organización

`AWSConfigMultiAccountSetupPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de junio de 2019 a las 18:03 UTC
- Hora de edición: 24 de febrero de 2023 a las 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigRemediationServiceRolePolicy

Descripción: Permite a AWS Config corregir los recursos no conformes en su nombre.

`AWSConfigRemediationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de junio de 2019 a las 21:21 UTC
- Hora de edición: 18 de junio de 2019 a las 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigRoleForOrganizations

Descripción: Permite que AWS Config llame a Organizations de solo lectura AWS APIs

`AWSConfigRoleForOrganizations` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSConfigRoleForOrganizations` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 19 de marzo de 2018 a las 22:53 UTC
- Hora de edición: 24 de noviembre de 2020 a las 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigRulesExecutionRole

Descripción: Permite que una función de AWS Lambda acceda a la API de AWS Config y a las instantáneas de configuración que AWS Config entrega periódicamente a Amazon S3. Los roles que evalúan los cambios de configuración de las reglas personalizadas de Config requieren este acceso.

`AWSConfigRulesExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSConfigRulesExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de marzo de 2016 a las 17:59 UTC
- Hora de edición: 13 de mayo de 2019 a las 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigServiceRolePolicy

Descripción: Permite a Config llamar a AWS los servicios y recopilar configuraciones de recursos en su nombre.

`AWSConfigServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de mayo de 2018 a las 23:31 UTC

- Hora editada: 20 de junio de 2025 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Versión de la política

Versión de la política: v59 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
```

```
        "amplifyuibuilder:GetTheme",
        "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:GetEventIntegration",
        "app-integrations:ListApplications",
        "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",
        "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:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
```

```
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "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:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
```

```
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock: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:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
```

```
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
```

```
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "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:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
```

```
        "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:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
```

```
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "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",
        "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:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "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:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
```

```
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "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:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "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: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:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
```

```
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "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:ListExperimentTemplates",
        "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: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:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
```

```
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
```

```
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "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:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
```

```
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "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:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
```

```
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "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:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
```

```
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "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",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "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:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "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:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "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:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "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:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
```

```
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "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",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
```

```
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "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:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "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:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:ListChannels",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "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",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
```

```
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "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:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "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:GetDirectoryRegistration",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
```

```
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "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:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
```

```
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "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",
        "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:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver: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:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
```

```
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "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:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
```

```
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
```

```
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "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:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
```

```
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "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:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetServiceSetting",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
```

```
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "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",
        "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:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
```

```
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListServiceNetworks",
        "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:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "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:*::/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:*::/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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConfigUserAccess

Descripción: proporciona acceso para usar AWS Config, incluida la búsqueda por etiquetas en los recursos y la lectura de todas las etiquetas. Esto no proporciona permiso para configurar AWS Config, que requiere privilegios administrativos.

`AWSConfigUserAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSConfigUserAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de febrero de 2015 a las 19:38 UTC
- Hora de edición: 18 de marzo de 2019 a las 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSConnector

Descripción: Permite un amplio read/write acceso a TODOS los EC2 objetos, el read/write acceso a los depósitos de S3 que comiencen por «import-to-ec2» y la posibilidad de enumerar todos los cubos de S3 para que el AWS Conector los importe VMs en su nombre.

`AWSConnector` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSConnector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 11 de febrero de 2015 a las 17:14 UTC
- Hora de edición: 28 de septiembre de 2015 a las 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSControlTowerAccountServiceRolePolicy

Descripción: Permite a AWS Control Tower llamar a AWS servicios que proporcionan una configuración de cuentas automatizada y un gobierno centralizado en su nombre.

`AWSControlTowerAccountServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de junio de 2023 a las 22:04 UTC
- Hora editada: 3 de junio de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSControlTowerServiceRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por la Torre AWS de Control

`AWSControlTowerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSControlTowerServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 3 de mayo de 2019 a las 18:19 UTC
- Hora editada: 13 de enero de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSCostAndUsageReportAutomationPolicy

Descripción: concede permisos para describir la organización de la cuenta, crear buckets de S3 para el programa MAP y aplicarle etiquetas, crear un informe de costos y uso, y describir las definiciones de los informes de costo y uso.

`AWSCostAndUsageReportAutomationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSCostAndUsageReportAutomationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de noviembre de 2021 a las 21:27 UTC
- Hora de edición: 1 de noviembre de 2021 a las 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeDataGrantOwnerFullAccess

Descripción: Da a los propietarios de Data Grant acceso a las acciones de AWS Data Exchange mediante el SDK AWS Management Console y.

`AWSDataExchangeDataGrantOwnerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeDataGrantOwnerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de octubre de 2024 a las 14:43 h UTC
- Hora de edición: 24 de octubre de 2024 a las 14:43 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeDataGrantReceiverFullAccess

Descripción: Da acceso al receptor de Data Grant a las acciones de AWS Data Exchange mediante el SDK AWS Management Console y.

`AWSDataExchangeDataGrantReceiverFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeDataGrantReceiverFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de octubre de 2024 a las 14:45 h UTC
- Hora de edición: 24 de octubre de 2024 a las 14:45 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeFullAccess

Descripción: Otorga acceso completo a AWS Data Exchange y a AWS Marketplace las acciones mediante el SDK AWS Management Console y. También proporciona un acceso selecto a los servicios relacionados necesarios para aprovechar al máximo las ventajas de AWS Data Exchange.

`AWSDataExchangeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 24 de junio de 2024 a las 19:54 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeProviderFullAccess

Descripción: Otorga al proveedor de datos acceso a AWS Data Exchange y a AWS Marketplace las acciones mediante el SDK AWS Management Console y. También proporciona un acceso selecto a los servicios relacionados necesarios para aprovechar al máximo las ventajas de AWS Data Exchange.

`AWSDataExchangeProviderFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeProviderFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 15 de agosto de 2024 a las 17:32 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeReadOnly

Descripción: Otorga acceso de solo lectura a AWS Data Exchange y a AWS Marketplace las acciones mediante el SDK AWS Management Console y.

`AWSDataExchangeReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 24 de octubre de 2024 a las 14:40 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeServiceRolePolicyForLicenseManagement

Descripción: Permite a AWS Data Exchange acceder a Servicios de AWS los recursos utilizados o gestionados por AWS Data Exchange para la gestión de licencias.

`AWSDataExchangeServiceRolePolicyForLicenseManagement` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de octubre de 2024 a las 14:54 h UTC
- Hora de edición: 10 de octubre de 2024 a las 14:54 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Descripción: Permite a AWS Data Exchange leer datos sobre su AWS organización para determinar si reúne los requisitos para AWS la distribución de licencias de concesión de datos de Data Exchange.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de octubre de 2024 a las 14:33 h UTC
- Hora de edición: 10 de octubre de 2024 a las 14:33 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataExchangeSubscriberFullAccess

Descripción: Concede a los suscriptores de datos acceso a AWS Data Exchange y a AWS Marketplace las acciones mediante el SDK AWS Management Console y. También proporciona un acceso selecto a los servicios relacionados necesarios para aprovechar al máximo las ventajas de AWS Data Exchange.

`AWSDataExchangeSubscriberFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataExchangeSubscriberFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2019 a las 19:27 UTC
- Hora de edición: 21 de mayo de 2024 a las 17:36 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataLifecycleManagerServiceRole

Descripción: Proporciona los permisos adecuados a AWS Data Lifecycle Manager para que tome medidas con respecto a AWS los recursos

`AWSDataLifecycleManagerServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataLifecycleManagerServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de julio de 2018 a las 19:34 UTC
- Hora editada: 16 de diciembre de 2024 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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.*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataLifecycleManagerServiceRoleForAMIManagement

Descripción: Proporciona los permisos adecuados a AWS Data Lifecycle Manager para que tome medidas con respecto a los AWS recursos de la administración de la AMI

`AWSDataLifecycleManagerServiceRoleForAMIManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataLifecycleManagerServiceRoleForAMIManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 21 de octubre de 2020 a las 19:39 UTC
- Hora de edición: 19 de agosto de 2021 a las 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataLifecycleManagerSSMFullAccess

Descripción: Proporciona permiso a Amazon Data Lifecycle Manager para realizar las acciones de Systems Manager necesarias para ejecutar scripts previos y posteriores en todas las EC2 instancias de Amazon.

`AWSDataLifecycleManagerSSMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataLifecycleManagerSSMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 31 de octubre de 2023 a las 20:29 UTC
- Hora de edición: 16 de noviembre de 2023 a las 22:31 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataPipeline_FullAccess

Descripción: proporciona acceso completo a Data Pipeline, acceso a listas para S3, DynamoDB, Redshift, RDS, SNS y roles de IAM, y acceso passRole para roles predeterminados.

`AWSDataPipeline_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataPipeline_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de enero de 2017 a las 23:14 UTC

- Hora de edición: 17 de agosto de 2017 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataPipeline_PowerUser

Descripción: proporciona acceso completo a Data Pipeline, acceso a listas para S3, DynamoDB, Redshift, RDS, SNS y roles de IAM, y acceso passRole para roles predeterminados.

`AWSDataPipeline_PowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataPipeline_PowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de enero de 2017 a las 23:16 UTC
- Hora de edición: 17 de agosto de 2017 a las 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataSyncDiscoveryServiceRolePolicy

Descripción: Permite que DataSync Discovery se integre con otros AWS servicios en su nombre.

`AWSDataSyncDiscoveryServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de marzo de 2023 a las 22:19 UTC
- Hora de edición: 20 de marzo de 2023 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataSyncFullAccess

Descripción: Proporciona acceso total AWS DataSync y acceso mínimo a sus dependencias

`AWSDataSyncFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataSyncFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de enero de 2019 a las 19:40 UTC
- Hora editada: 20 de mayo de 2025 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Versión de la política

Versión de la política: v10 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataSyncReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS DataSync

`AWSDataSyncReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDataSyncReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 18 de enero de 2019 a las 19:18 UTC
- Hora de edición: 30 de junio de 2020 a las 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDataSyncServiceRolePolicy

Descripción: Permite DataSync integrarse con otros AWS servicios en su nombre

`AWSDataSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 09 de octubre de 2024 a las 17:45 h UTC
- Hora editada: 15 de abril de 2025 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-FleetWorker

Descripción: Proporciona a los trabajadores de AWS Deadline Cloud acceso para ejecutar tareas en una granja.

`AWSDeadlineCloud-FleetWorker` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-FleetWorker` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 01 de abril de 2024 a las 17:21 h UTC
- Hora de edición: 01 de abril de 2024 a las 17:21 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-UserAccessFarms

Descripción: Proporciona a los usuarios acceso a las estaciones de trabajo de los usuarios a las granjas de AWS Deadline Cloud con permisos limitados de solo lectura para llamar a otros servicios necesarios. Asociar esta política al rol de usuario asociado al estudio.

`AWSDeadlineCloud-UserAccessFarms` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-UserAccessFarms` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 01 de abril de 2024 a las 16:54 h UTC
- Hora de edición: 07 de octubre de 2024 a las 17:57 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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: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: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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-UserAccessFleets

Descripción: Proporciona a los usuarios acceso a las estaciones de trabajo de los usuarios a las flotas de AWS Deadline Cloud con permisos limitados de solo lectura para llamar a otros servicios necesarios. Asociar esta política al rol de usuario asociado al estudio.

`AWSDeadlineCloud-UserAccessFleets` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-UserAccessFleets` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 01 de abril de 2024 a las 17:01 h UTC
- Hora de edición: 01 de abril de 2024 a las 17:01 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:GetWorker",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "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}"
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-UserAccessJobs

Descripción: Proporciona a los usuarios acceso desde la estación de trabajo a los trabajos de AWS Deadline Cloud con permisos limitados de solo lectura para llamar a otros servicios necesarios. Asociar esta política al rol de usuario asociado al estudio.

`AWSDeadlineCloud-UserAccessJobs` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-UserAccessJobs` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 01 de abril de 2024 a las 17:05 h UTC
- Hora de edición: 07 de octubre de 2024 a las 18:24 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-UserAccessQueues

Descripción: Proporciona a los usuarios acceso desde las estaciones de trabajo a las colas de AWS Deadline Cloud con permisos limitados de solo lectura para llamar a otros servicios necesarios. Asociar esta política al rol de usuario asociado al estudio.

`AWSDeadlineCloud-UserAccessQueues` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-UserAccessQueues` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 01 de abril de 2024 a las 17:10 h UTC
- Hora de edición: 07 de octubre de 2024 a las 18:25 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeadlineCloud-WorkerHost

Descripción: Proporciona acceso a los trabajadores anfitriones de AWS Deadline Cloud para unirse a una flota en una granja.

`AWSDeadlineCloud-WorkerHost` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeadlineCloud-WorkerHost` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 01 de abril de 2024 a las 17:28 h UTC
- Hora editada: 30 de abril de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepLensLambdaFunctionAccessPolicy

Descripción: Esta política especifica los permisos que requieren las funciones lambda DeepLens administrativas que se ejecutan en un dispositivo DeepLens

`AWSDeepLensLambdaFunctionAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepLensLambdaFunctionAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 15:47 UTC
- Hora de edición: 11 de junio de 2019 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepLensServiceRolePolicy

Descripción: Otorga AWS DeepLens acceso a Servicios de AWS los recursos y las funciones que necesitan DeepLens y sus dependencias, incluidos IoT, S3 GreenGrass y AWS Lambda.

`AWSDeepLensServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepLensServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 29 de noviembre de 2017 a las 15:46 UTC
- Hora de edición: 25 de septiembre de 2019 a las 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerAccountAdminAccess

Descripción: acceso de DeepRacer administrador a todas las acciones, incluida la posibilidad de cambiar entre el modo multiusuario y el modo de usuario único.

`AWSDeepRacerAccountAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerAccountAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 28 de octubre de 2021 a las 01:27 UTC
- Hora de edición: 28 de octubre de 2021 a las 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerCloudFormationAccessPolicy

Descripción: Permite CloudFormation crear y gestionar AWS pilas y recursos en su nombre.

`AWSDeepRacerCloudFormationAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerCloudFormationAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de febrero de 2019 a las 21:59 UTC
- Hora de edición: 14 de junio de 2019 a las 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerDefaultMultiUserAccess

Descripción: Acceso de usuario DeepRacer MultiUser predeterminado para usar deepracer en modo multiusuario

`AWSDeepRacerDefaultMultiUserAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerDefaultMultiUserAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 28 de octubre de 2021 a las 01:27 UTC
- Hora de edición: 28 de octubre de 2021 a las 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerFullAccess

Descripción: Proporciona acceso completo a AWS DeepRacer. También, brinda acceso selecto a servicios relacionados (por ejemplo, S3).

`AWSDeepRacerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de octubre de 2020 a las 22:03 UTC
- Hora de edición: 5 de octubre de 2020 a las 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerRoboMakerAccessPolicy

Descripción: Permite RoboMaker crear los recursos necesarios y llamar a AWS los servicios en su nombre.

`AWSDeepRacerRoboMakerAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerRoboMakerAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de febrero de 2019 a las 21:59 UTC
- Hora de edición: 28 de febrero de 2019 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeepRacerServiceRolePolicy

Descripción: Permite DeepRacer crear los recursos necesarios y llamar a AWS los servicios en su nombre.

`AWSDeepRacerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeepRacerServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 28 de febrero de 2019 a las 21:58 UTC
- Hora de edición: 12 de junio de 2019 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDenyAll

Descripción: denegar todo el acceso.

`AWSDenyAll` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDenyAll` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de mayo de 2019 a las 22:36 UTC
- Hora de edición: 18 de diciembre de 2023 a las 16:42 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeviceFarmFullAccess

Descripción: Proporciona acceso completo a todas las operaciones de AWS Device Farm.

`AWSDeviceFarmFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDeviceFarmFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de julio de 2015 a las 16:37 UTC
- Hora de edición: 13 de julio de 2015 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeviceFarmServiceRolePolicy

Descripción: Otorgue permisos a AWS Device Farm para que llame a EC2 Network APIs en su nombre.

`AWSDeviceFarmServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de septiembre de 2022 a las 21:02 UTC
- Hora de edición: 20 de septiembre de 2022 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDeviceFarmTestGridServiceRolePolicy

Descripción: Concede permisos a AWS Device Farm para que llame EC2 APIs en tu nombre.

`AWSDeviceFarmTestGridServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de mayo de 2021 a las 22:01 UTC
- Hora de edición: 26 de mayo de 2021 a las 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectConnectFullAccess

Descripción: Proporciona acceso completo a AWS Direct Connect a través de AWS Management Console.

`AWSDirectConnectFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectConnectFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 30 de abril de 2019 a las 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectConnectReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Direct Connect a través de AWS Management Console.

`AWSDirectConnectReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectConnectReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC

- Hora de edición: 18 de mayo de 2020 a las 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectConnectServiceRolePolicy

Descripción: Proporciona permiso de AWS Direct Connect para crear y administrar AWS recursos en su nombre.

`AWSDirectConnectServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de enero de 2021 a las 18:35 UTC
- Hora de edición: 14 de enero de 2021 a las 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
```

```
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectoryServiceDataFullAccess

Descripción: Proporciona acceso completo a los datos AWS del Directory Service.

`AWSDirectoryServiceDataFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectoryServiceDataFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de septiembre de 2024 a las 21:45 h UTC
- Hora de edición: 18 de septiembre de 2024 a las 21:45 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectoryServiceDataReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los datos del AWS Directory Service

`AWSDirectoryServiceDataReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectoryServiceDataReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 18 de septiembre de 2024 a las 22:00 h UTC
- Hora de edición: 18 de septiembre de 2024 a las 22:00 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectoryServiceFullAccess

Descripción: Proporciona acceso completo a AWS Directory Service.

`AWSDirectoryServiceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectoryServiceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 02 de abril de 2024 a las 20:38 h UTC

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

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDirectoryServiceReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDirectoryServiceReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 25 de septiembre de 2018 a las 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDiscoveryContinuousExportFirehosePolicy

Descripción: Proporciona acceso de escritura a AWS los recursos necesarios para AWS Discovery Continuous Export

`AWSDiscoveryContinuousExportFirehosePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSDiscoveryContinuousExportFirehosePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de agosto de 2018 a las 18:29 UTC
- Hora de edición: 8 de junio de 2021 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDMSFleetAdvisorServiceRolePolicy

Descripción: Permite a DMS Fleet Advisor gestionar CloudWatch las métricas en su nombre.

`AWSDMSFleetAdvisorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de marzo de 2023 a las 09:10 UTC
- Hora de edición: 6 de marzo de 2023 a las 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSDMSServerlessServiceRolePolicy

Descripción: Otorga a AWS DMS permisos sin servidor para crear y administrar los recursos de DMS en su cuenta en su nombre

`AWSDMSServerlessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de mayo de 2023 a las 20:28 UTC
- Hora de edición: 7 de febrero de 2025 a las 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ],
      "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-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEC2CapacityReservationFleetRolePolicy

Descripción: Permite que EC2 CapacityReservation Fleet Service gestione las reservas de capacidad

`AWSEC2CapacityReservationFleetRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de septiembre de 2021 a las 14:43 UTC
- Hora editada: 3 de marzo de 2025 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEC2FleetServiceRolePolicy

Descripción: Permite a EC2 Fleet lanzar y gestionar instancias.

`AWSEC2FleetServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de marzo de 2018 a las 00:08 UTC
- Hora de edición: 4 de mayo de 2020 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEC2SpotFleetServiceRolePolicy

Descripción: Permite a EC2 Spot Fleet lanzar y gestionar instancias de flota puntual

`AWSEC2SpotFleetServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de octubre de 2017 a las 19:13 UTC

- Hora de edición: 16 de marzo de 2020 a las 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEC2SpotServiceRolePolicy

Descripción: Permite a EC2 Spot lanzar y gestionar instancias puntuales

`AWSEC2SpotServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2017 a las 18:51 UTC
- Hora de edición: 12 de diciembre de 2018 a las 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEC2VssSnapshotPolicy

Descripción: Esta política se adjunta a la función de IAM asociada a sus instancias de Amazon EC2 Windows para permitir que la solución Amazon EC2 VSS cree y añada etiquetas a Amazon Machine Images (AMI) y a las instantáneas de EBS.

`AWSEC2VssSnapshotPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSEC2VssSnapshotPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 27 de marzo de 2024 a las 16:32 h UTC
- Hora editada: 20 de noviembre de 2024 a las 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSECRPullThroughCache_ServiceRolePolicy

Descripción: Permite el acceso a AWS los servicios y recursos utilizados o administrados por la memoria caché de extracción de AWS ECR

`AWSECRPullThroughCache_ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2021 a las 21:51 UTC
- Hora editada: 6 de marzo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkCustomPlatformforEC2Role

Descripción: Proporcione permiso a la instancia en su entorno de creación de plataformas personalizado para lanzar la EC2 instancia, crear una instantánea y una AMI de EBS, transmitir registros a Amazon CloudWatch Logs y almacenar artefactos en Amazon S3.

`AWSElasticBeanstalkCustomPlatformforEC2Role` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkCustomPlatformforEC2Role` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de febrero de 2017 a las 22:50 UTC
- Hora de edición: 21 de febrero de 2017 a las 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkEnhancedHealth

Descripción: Política de AWS Elastic Beanstalk Service para el sistema Health Monitoring

`AWSElasticBeanstalkEnhancedHealth` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkEnhancedHealth` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de febrero de 2016 a las 23:17 UTC
- Hora de edición: 9 de abril de 2018 a las 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkMaintenance

Descripción: AWS Política de rol de servicio de Elastic Beanstalk que otorga permisos limitados para actualizar sus recursos en su nombre con fines de mantenimiento.

`AWSElasticBeanstalkMaintenance` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 11 de enero de 2019 a las 23:22 UTC
- Hora de edición: 29 de abril de 2024 a las 21:48 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Descripción: Esta política es para el rol de servicio de AWS Elastic Beanstalk que se utiliza para realizar actualizaciones administradas de los entornos de Elastic Beanstalk. Esta política no debe asociarse a otros usuarios o roles. La política otorga amplios permisos para crear y administrar recursos en varios AWS servicios AutoScaling, incluidos ECS EC2, Elastic Load Balancing y CloudFormation. Esta política también permite transferir cualquier rol de IAM que pueda utilizarse con esos servicios.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de marzo de 2021 a las 22:18 UTC
- Hora editada: 27 de febrero de 2025 a las 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Descripción: AWS Política de rol de servicio de Elastic Beanstalk que otorga permisos limitados a las actualizaciones administradas.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de noviembre de 2019 a las 22:35 UTC
- Hora de edición: 29 de abril de 2024 a las 23:11 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkMulticontainerDocker

Descripción: Proporcione acceso a las instancias de su entorno Docker multicontenedor para utilizar Amazon EC2 Container Service a fin de gestionar las tareas de despliegue de contenedores.

`AWSElasticBeanstalkMulticontainerDocker` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkMulticontainerDocker` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de febrero de 2016 a las 23:15 UTC
- Hora de edición: 23 de marzo de 2023 a las 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkReadOnly

Descripción: concede permisos de solo lectura. Permite explícitamente a los operadores obtener acceso directo para recuperar información sobre los recursos relacionados con las aplicaciones de AWS Elastic Beanstalk.

`AWSElasticBeanstalkReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de enero de 2021 a las 19:02 UTC
- Hora de edición: 22 de enero de 2021 a las 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleCore

Descripción: AWSElastic BeanstalkRoleCore (función de operaciones de Elastic Beanstalk) Permite el funcionamiento principal de un entorno de servicios web.

`AWSElasticBeanstalkRoleCore` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleCore` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:48 UTC
- Hora de edición: 30 de abril de 2024 a las 00:01 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleCWL

Descripción: (función de operaciones de Elastic Beanstalk) Permite que un entorno administre CloudWatch grupos de registros de Amazon Logs.

`AWSElasticBeanstalkRoleCWL` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleCWL` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:49 UTC
- Hora de edición: 5 de junio de 2020 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleECS

Descripción: (rol de operaciones de Elastic Beanstalk) permite que un entorno de múltiples contenedores de Docker administre los clústeres de Amazon ECS.

`AWSElasticBeanstalkRoleECS` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleECS` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:47 UTC
- Hora de edición: 23 de marzo de 2023 a las 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleRDS

Descripción: (rol de operaciones de Elastic Beanstalk) permite que un entorno integre una instancia de Amazon RDS.

`AWSElasticBeanstalkRoleRDS` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleRDS` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:46 UTC
- Hora de edición: 5 de junio de 2020 a las 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleSNS

Descripción: (rol de operaciones de Elastic Beanstalk) permite que un entorno habilite una integración de un tema de Amazon SNS.

`AWSElasticBeanstalkRoleSNS` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleSNS` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:46 UTC
- Hora de edición: 5 de junio de 2020 a las 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkRoleWorkerTier

Descripción: (el rol de operaciones de Elastic Beanstalk) permite que un nivel de entorno de trabajo cree una tabla de Amazon DynamoDB y una cola de Amazon SQS.

`AWSElasticBeanstalkRoleWorkerTier` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkRoleWorkerTier` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2020 a las 21:43 UTC
- Hora de edición: 5 de junio de 2020 a las 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkService

Descripción: esta política está en proceso de quedar obsoleta. Consulte la documentación para obtener orientación: https://docs.aws.amazon.com/elasticbeanstalk/ latest/dg/iam -servicerole.html. AWS Política de roles de Elastic Beanstalk Service que otorga permisos para crear y administrar recursos (AutoScalinges decir EC2,, CloudFormation S3, ELB, etc.) en su nombre.

`AWSElasticBeanstalkService` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkService` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de abril de 2016 a las 20:27 UTC
- Hora de edición: 10 de mayo de 2023 a las 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Versión de la política

Versión de la política: v17 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkServiceRolePolicy

Descripción: AWS Política de roles vinculados del servicio de Elastic Beanstalk que otorga permisos para crear y administrar recursos (AutoScalinges decir EC2, CloudFormation S3, ELB, etc.) en su nombre.

`AWSElasticBeanstalkServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de septiembre de 2017 a las 23:46 UTC
- Hora de edición: 6 de junio de 2019 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkWebTier

Descripción: proporciona a las instancias del entorno de servidor web acceso para cargar archivos de registro en Amazon S3.

`AWSElasticBeanstalkWebTier` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkWebTier` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 8 de febrero de 2016 a las 23:08 UTC
- Hora de edición: 9 de septiembre de 2020 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticBeanstalkWorkerTier

Descripción: Proporcione acceso a las instancias de su entorno de trabajo para cargar archivos de registro en Amazon S3, utilizar Amazon SQS para supervisar la cola de trabajos de su solicitud, utilizar Amazon DynamoDB para elegir líderes y a Amazon para publicar métricas para la supervisión del estado. CloudWatch

`AWSElasticBeanstalkWorkerTier` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticBeanstalkWorkerTier` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de febrero de 2016 a las 23:12 UTC
- Hora de edición: 9 de septiembre de 2020 a las 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryAgentInstallationPolicy

Descripción: Esta política permite instalar el agente de AWS replicación, que se usa con AWS Elastic Disaster Recovery (DRS) para recuperar servidores externos AWS. Adjunte esta política a los usuarios o roles de IAM cuyas credenciales proporcione durante el paso de instalación del agente de AWS replicación.

`AWSElasticDisasterRecoveryAgentInstallationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryAgentInstallationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2021 a las 10:37 UTC
- Hora de edición: 27 de noviembre de 2023 a las 12:38 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryAgentPolicy

Descripción: Esta política permite usar el agente de AWS replicación, que se usa con AWS Elastic Disaster Recovery (DRS) para recuperar los servidores de origen AWS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryAgentPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryAgentPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:32 UTC

- Hora de edición: 27 de noviembre de 2023 a las 13:44 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryConsoleFullAccess

Descripción: Esta política proporciona acceso total a todo el público APIs de AWS Elastic Disaster Recovery (DRS), así como permisos para leer la clave de KMS, License Manager, Resource Groups, Elastic Load Balancing, IAM e EC2 información. Asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2021 a las 10:46 UTC
- Hora editada: 12 de enero de 2025 a las 07:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Descripción: Esta política proporciona acceso total a todos los usuarios públicos APIs de AWS Elastic Disaster Recovery (AWS DRS), así como a todos los demás AWS servicios públicos APIs utilizados por AWS DRS Console. Asocie esta política a los usuarios o roles.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryConsoleFullAccess_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2023 a las 13:35 h UTC
- Hora editada: 2 de julio de 2025 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Versión de la política

Versión de la política: v5 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : {
        "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/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
```

```
            "CreateNetworkInterface"
          ]
        },
        "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" : [
        "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/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" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "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" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryConversionServerPolicy

Descripción: Esta política se adjunta a la función de instancia del servidor de conversión de AWS Elastic Disaster Recovery. Esta política permite que los servidores de conversión de Elastic Disaster Recovery (DRS), que son EC2 instancias lanzadas por Elastic Disaster Recovery, se comuniquen con el servicio DRS. DRS asigna una función de IAM con esta política (como perfil de

EC2 instancia) a los servidores de conversión de DRS, que DRS lanza y termina automáticamente cuando es necesario. No es recomendable que asocie esta política a sus usuarios o roles de IAM. La Recuperación de desastres Elastic utiliza los Servidores de conversión DRS cuando los usuarios eligen recuperar los servidores de origen mediante la consola, la CLI o la API de DRS.

`AWSElasticDisasterRecoveryConversionServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryConversionServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 13:42 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:13 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Descripción: Esta política permite a AWS Elastic Disaster Recovery (DRS) admitir la replicación entre cuentas y la conmutación por recuperación entre cuentas.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de mayo de 2023 a las 07:16 UTC
- Hora de edición: 17 de enero de 2024 a las 13:19 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryEc2InstancePolicy

Descripción: Esta política permite instalar y usar el agente de AWS replicación, que AWS Elastic Disaster Recovery (DRS) utiliza para recuperar los servidores de origen que se ejecutan en ellos EC2 (entre regiones o entre zonas de disponibilidad). Se debe adjuntar a las instancias una función de IAM con esta política (como perfil de EC2 instancia). EC2

`AWSElasticDisasterRecoveryEc2InstancePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryEc2InstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de mayo de 2022 a las 12:30 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:39 h UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Descripción: Puede adjuntar la AWSElastic DisasterRecoveryFailbackInstallationPolicy política a sus identidades de IAM. Esta política permite instalar el cliente de conmutación por recuperación de la Recuperación de desastres Elastic, que se utiliza para devolver las instancias de recuperación a la infraestructura de origen original. Asocie esta política a los usuarios o roles de IAM cuyas credenciales proporciona al ejecutar el cliente de conmutación por recuperación de la Recuperación de desastres Elastic.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryFailbackInstallationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2021 a las 11:02 UTC

- Hora de edición: 27 de noviembre de 2023 a las 13:43 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryFailbackPolicy

Descripción: esta política permite utilizar el cliente de conmutación por recuperación de la Recuperación elástica ante desastres, que se utiliza para conmutar por recuperación las instancias de recuperación a la infraestructura de origen inicial. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryFailbackPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryFailbackPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:41 UTC
- Hora de edición: 27 de noviembre de 2023 a las 12:56 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryLaunchActionsPolicy

Descripción: Esta política le permite usar Amazon SSM y los permisos necesarios para ejecutar acciones posteriores al lanzamiento en AWS Elastic Disaster Recovery (AWS DRS). Asocie esta política a sus roles o usuarios de IAM.

`AWSElasticDisasterRecoveryLaunchActionsPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryLaunchActionsPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 13 de septiembre de 2023 a las 07:38 UTC

- Hora editada: 2 de julio de 2025 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/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/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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Descripción: Esta política permite que AWS Elastic Disaster Recovery (DRS) admita la replicación de la red.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryNetworkReplicationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de junio de 2023 a las 12:36 UTC

- Hora de edición: 02 de enero de 2024 a las 13:25 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryReadOnlyAccess

Descripción: Puede adjuntar la AWSElastic DisasterRecoveryReadOnlyAccess política a sus identidades de IAM. Esta política proporciona permisos a todos los servicios públicos APIs de solo lectura de Elastic Disaster Recovery (DRS), así como a algunos otros AWS servicios APIs de solo lectura que se requieren para poder utilizar completamente la consola de DRS en modo de solo lectura. Asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2021 a las 10:50 UTC
- Hora de edición: 29 de julio de 2024 a las 19:39 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Descripción: esta política está asociada al rol de instancia de la instancia de recuperación de Recuperación elástica ante desastres. Esta política permite que las instancias de recuperación de Elastic Disaster Recovery (DRS), que son EC2 instancias lanzadas por Elastic Disaster Recovery, se comuniquen con el servicio DRS y puedan volver a su infraestructura de origen original. Elastic Disaster Recovery asigna una función de IAM con esta política (como perfil de EC2 instancia) a las instancias de recuperación de DRS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryRecoveryInstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:20 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:11 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryReplicationServerPolicy

Descripción: esta política está asociada al rol de instancia del servidor de replicación de Recuperación elástica ante desastres. Esta política permite que los servidores de replicación de Elastic Disaster Recovery (DRS), que son EC2 instancias lanzadas por Elastic Disaster Recovery, se comuniquen con el servicio DRS y creen instantáneas de EBS en sus servidores. Cuenta de AWS Elastic Disaster Recovery asigna una función de IAM con esta política (como perfil de EC2 instancia) a los servidores de replicación de DRS, que DRS lanza y termina automáticamente, según sea necesario. Los servidores de replicación DRS se utilizan para facilitar la replicación de datos desde sus servidores externos AWS, como parte del proceso de recuperación gestionado por DRS. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryReplicationServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryReplicationServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de noviembre de 2021 a las 13:34 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:28 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryServiceRolePolicy

Descripción: Esta política permite a Elastic Disaster Recovery administrar AWS los recursos en su nombre.

`AWSElasticDisasterRecoveryServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 10:56 UTC
- Hora de edición: 5 de enero de 2025 a las 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryStagingAccountPolicy

Descripción: Esta política permite el acceso de solo lectura a los recursos de AWS Elastic Disaster Recovery (DRS), como los servidores de origen y los trabajos. También, permite crear una captura convertida y compartirla con una cuenta específica.

`AWSElasticDisasterRecoveryStagingAccountPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryStagingAccountPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de mayo de 2022 a las 09:49 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:07 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Descripción: AWS Elastic Disaster Recovery (DRS) utiliza esta política para recuperar los servidores de origen en una cuenta de destino independiente y permitir la recuperación de errores. No es recomendable que asocie esta política a sus usuarios o roles de IAM.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de enero de 2023 a las 12:11 UTC
- Hora de edición: 27 de noviembre de 2023 a las 13:32 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticLoadBalancingClassicServiceRolePolicy

Descripción: Política de funciones vinculadas al servicio para AWS Elastic Load Balancing Control Plane (Classic)

`AWSElasticLoadBalancingClassicServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de septiembre de 2017 a las 22:36 UTC
- Hora de edición: 7 de octubre de 2019 a las 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElasticLoadBalancingServiceRolePolicy

Descripción: Política de funciones vinculadas a servicios para el plano de control de AWS Elastic Load Balancing

`AWSElasticLoadBalancingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de septiembre de 2017 a las 22:19 UTC
- Hora de edición: 17 de febrero de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaConnectFullAccess

Descripción: Proporciona acceso completo a los MediaConnect recursos de AWS Elemental.

`AWSElementalMediaConnectFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaConnectFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de febrero de 2025 a las 20:07 UTC
- Hora editada: 12 de febrero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaConnectReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los recursos de AWS Elemental MediaConnect .

`AWSElementalMediaConnectReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaConnectReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 12 de febrero de 2025 a las 20:07 UTC
- Hora editada: 12 de febrero de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaConvertFullAccess

Descripción: Proporciona acceso completo a AWS Elemental MediaConvert a través del SDK AWS Management Console y.

`AWSElementalMediaConvertFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaConvertFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de junio de 2018 a las 19:25 UTC
- Hora de edición: 10 de junio de 2019 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaConvertReadOnly

Descripción: Proporciona acceso de solo lectura a AWS Elemental MediaConvert a través del AWS Management Console SDK.

`AWSElementalMediaConvertReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaConvertReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de junio de 2018 a las 19:25 UTC
- Hora de edición: 10 de junio de 2019 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaLiveFullAccess

Descripción: Proporciona acceso completo a los MediaLive recursos de AWS Elemental

`AWSElementalMediaLiveFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaLiveFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de julio de 2020 a las 17:07 UTC
- Hora de edición: 8 de julio de 2020 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaLiveReadOnly

Descripción: Proporciona acceso de solo lectura a los MediaLive recursos de AWS Elemental

`AWSElementalMediaLiveReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaLiveReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de julio de 2020 a las 16:38 UTC
- Hora de edición: 22 de julio de 2024 a las 17:08 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSElementalMediaLiveReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "medialive:Get*",
```

```
        "medialive:List*",
        "medialive:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaPackageFullAccess

Descripción: Proporciona acceso completo a los MediaPackage recursos de AWS Elemental

`AWSElementalMediaPackageFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaPackageFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de diciembre de 2017 a las 23:39 UTC
- Hora de edición: 29 de diciembre de 2017 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaPackageReadOnly

Descripción: Proporciona acceso de solo lectura a los MediaPackage recursos de AWS Elemental

`AWSElementalMediaPackageReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaPackageReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de diciembre de 2017 a las 00:04 UTC

- Hora de edición: 30 de diciembre de 2017 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaPackageV2FullAccess

Descripción: Proporciona acceso completo a los recursos de AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaPackageV2FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de julio de 2023 a las 20:29 UTC
- Hora de edición: 25 de julio de 2023 a las 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaPackageV2ReadOnly

Descripción: Proporciona acceso de solo lectura a los recursos de AWS Elemental MediaPackage V2.

`AWSElementalMediaPackageV2ReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaPackageV2ReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 25 de julio de 2023 a las 20:31 UTC
- Hora de edición: 25 de julio de 2023 a las 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaStoreFullAccess

Descripción: Proporciona acceso completo de lectura y escritura a todos MediaStore APIs

`AWSElementalMediaStoreFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaStoreFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de marzo de 2018 a las 23:15 UTC
- Hora de edición: 5 de marzo de 2018 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaStoreReadOnly

Descripción: Proporciona permisos de solo lectura para MediaStore APIs

`AWSElementalMediaStoreReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaStoreReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 8 de marzo de 2018 a las 19:48 UTC
- Hora de edición: 8 de marzo de 2018 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaTailorFullAccess

Descripción: Proporciona acceso completo a los MediaTailor recursos de AWS Elemental

`AWSElementalMediaTailorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaTailorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de noviembre de 2021 a las 00:04 UTC
- Hora de edición: 23 de noviembre de 2021 a las 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSElementalMediaTailorReadOnly

Descripción: Proporciona acceso de solo lectura a los MediaTailor recursos de AWS Elemental

`AWSElementalMediaTailorReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSElementalMediaTailorReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de noviembre de 2021 a las 00:05 UTC
- Hora de edición: 23 de noviembre de 2021 a las 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEnhancedClassicNetworkingMangementPolicy

Descripción: política para habilitar la característica de administración de redes clásica mejorada.

`AWSEnhancedClassicNetworkingMangementPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de septiembre de 2017 a las 17:29 UTC
- Hora de edición: 20 de septiembre de 2017 a las 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEntityResolutionConsoleFullAccess

Descripción: Proporciona acceso completo desde la consola a AWS Entity Resolution y a los servicios relacionados.

`AWSEntityResolutionConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSEntityResolutionConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de agosto de 2023 a las 17:54 UTC
- Hora de edición: 16 de octubre de 2023 a las 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSEntityResolutionConsoleReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Entity Resolution a través del. AWS Management Console

`AWSEntityResolutionConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSEntityResolutionConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 17 de agosto de 2023 a las 18:18 UTC
- Hora de edición: 17 de agosto de 2023 a las 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorEC2Access

Descripción: Esta política otorga permiso al servicio de simulador de inyección de fallas EC2 y otros servicios necesarios para realizar acciones de FIS.

`AWSFaultInjectionSimulatorEC2Access` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorEC2Access` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:39 UTC
- Hora editada: 12 de febrero de 2025 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorECSAccess

Descripción: esta política concede al Servicio de simulador de inyección de errores el permiso en ECS y otros servicios que se necesitan para realizar acciones del Simulador de inyección de errores.

`AWSFaultInjectionSimulatorECSAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorECSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:37 UTC
- Hora editada: 7 de marzo de 2025 a las 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorEKSAccess

Descripción: esta política concede al Servicio de simulador de inyección de errores el permiso en EKS y otros servicios que se necesitan para realizar acciones del Simulador de inyección de errores.

`AWSFaultInjectionSimulatorEKSAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorEKSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:34 UTC
- Hora editada: 11 de marzo de 2025 a las 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorNetworkAccess

Descripción: Esta política otorga al servicio de simulador de inyección de fallas permiso para EC2 utilizar redes y otros servicios necesarios para realizar acciones de FIS.

`AWSFaultInjectionSimulatorNetworkAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorNetworkAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:32 UTC
- Hora editada: 11 de marzo de 2025 a las 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorRDSAccess

Descripción: esta política concede al Servicio de simulador de inyección de errores el permiso en RDS y otros servicios que se necesitan para realizar acciones del Simulador de inyección de errores.

`AWSFaultInjectionSimulatorRDSAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorRDSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 20:30 UTC
- Hora editada: 18 de marzo de 2025 a las 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFaultInjectionSimulatorSSMAccess

Descripción: esta política concede al Servicio de simulador de inyección de errores el permiso en SSM y otros servicios que se necesitan para realizar acciones del Simulador de inyección de errores.

`AWSFaultInjectionSimulatorSSMAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFaultInjectionSimulatorSSMAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de octubre de 2022 a las 15:33 UTC
- Hora editada: 25 de junio de 2025 a las 14:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFinSpaceServiceRolePolicy

Descripción: Política para permitir el acceso a Servicio de AWS los recursos utilizados o gestionados por Amazon FinSpace

`AWSFinSpaceServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de mayo de 2023 a las 16:42 UTC
- Hora de edición: 01 de diciembre de 2023 a las 21:05 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFMAdminFullAccess

Descripción: Acceso completo para el administrador de AWS FM

`AWSFMAdminFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFMAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2018 a las 18:06 UTC
- Hora de edición: 20 de octubre de 2022 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFMAdminReadOnlyAccess

Descripción: Acceso de solo lectura para el administrador de AWS FM que permite monitorear las operaciones de AWS FM

`AWSFMAdminReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFMAdminReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2018 a las 20:07 UTC
- Hora de edición: 31 de octubre de 2022 a las 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSFMMemberReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a las acciones de AWS WAF para las cuentas de los miembros de AWS Firewall Manager

`AWSFMMemberReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSFMMemberReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2018 a las 21:05 UTC
- Hora de edición: 9 de mayo de 2018 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSForWordPressPluginPolicy

Descripción: Política gestionada para el complemento AWS For Wordpress

`AWSForWordPressPluginPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSForWordPressPluginPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de octubre de 2019 a las 00:27 UTC
- Hora de edición: 20 de enero de 2020 a las 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGitSyncServiceRolePolicy

Descripción: Política que permite a AWS Code Connections sincronizar el contenido de tu repositorio de git

`AWSGitSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2023 a las 17:05 UTC
- Hora de edición: 26 de abril de 2024 a las 18:12 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlobalAcceleratorSLRPolicy

Descripción: Política que otorga permisos a AWS Global Accelerator para administrar las interfaces de EC2 Elastic Network y los grupos de seguridad.

`AWSGlobalAcceleratorSLRPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de abril de 2019 a las 19:39 UTC

- Hora editada: 29 de octubre de 2024 a las 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueConsoleFullAccess

Descripción: Proporciona acceso completo a AWS Glue a través del AWS Management Console

`AWSGlueConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 14 de julio de 2023 a las 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueConsoleSageMakerNotebookFullAccess

Descripción: Proporciona acceso completo a AWS Glue a través de las instancias del cuaderno Sagemaker AWS Management Console y acceso a ellas.

`AWSGlueConsoleSageMakerNotebookFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueConsoleSageMakerNotebookFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de octubre de 2018 a las 17:52 UTC
- Hora de edición: 15 de julio de 2021 a las 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AwsGlueDataBrewFullAccessPolicy

Descripción: Proporciona acceso completo a AWS Glue DataBrew a través del AWS Management Console. También, proporciona acceso selecto a los servicios relacionados (por ejemplo, S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AwsGlueDataBrewFullAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de noviembre de 2020 a las 16:51 UTC
- Hora de edición: 4 de febrero de 2022 a las 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueDataBrewServiceRole

Descripción: esta política concede permiso a Glue para que realice acciones en el catálogo de datos de Glue del usuario. Esta política también concede permiso a EC2 acciones para permitir que Glue cree una interfaz de red elástica (ENI) para establecer conexión con los recursos de la VPC. Además, permite que Glue acceda a los datos registrados en Lake Formation, y concede permiso para acceder a CloudWatch del usuario

`AWSGlueDataBrewServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueDataBrewServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 4 de diciembre de 2020 a las 21:26 UTC
- Hora de edición: 20 de marzo de 2024 a las 23:28 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueSchemaRegistryFullAccess

Descripción: Proporciona acceso completo al servicio de registro de AWS Glue Schema

`AWSGlueSchemaRegistryFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueSchemaRegistryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2020 a las 00:19 UTC
- Hora de edición: 20 de noviembre de 2020 a las 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueSchemaRegistryReadonlyAccess

Descripción: Proporciona acceso de solo lectura al servicio de registro de AWS Glue Schema

`AWSGlueSchemaRegistryReadonlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueSchemaRegistryReadonlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2020 a las 00:20 UTC
- Hora de edición: 20 de noviembre de 2020 a las 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueServiceNotebookRole

Descripción: Política para el rol de servicio de AWS Glue que permite al cliente administrar el servidor portátil

`AWSGlueServiceNotebookRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueServiceNotebookRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 09 de octubre de 2023 a las 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGlueServiceRole

Descripción: Política para el rol de servicio AWS Glue que permite el acceso a servicios relacionados EC2, incluidos S3 y Cloudwatch Logs

`AWSGlueServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGlueServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:37 UTC
- Hora de edición: 11 de septiembre de 2023 a las 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AwsGlueSessionUserRestrictedNotebookPolicy

Descripción: proporciona permisos que permiten a los usuarios crear y utilizar únicamente las sesiones de bloc de notas asociadas al usuario. Esta política también incluye permisos para que los usuarios puedan pasar expresamente un rol de sesión de Glue restringido.

`AwsGlueSessionUserRestrictedNotebookPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedNotebookPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de abril de 2022 a las 15:24 UTC
- Hora de edición: 15 de agosto de 2024 a las 20:51 h UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AwsGlueSessionUserRestrictedNotebookServiceRole

Descripción: Proporciona acceso completo a todos los recursos de AWS Glue, excepto a las sesiones. Permite a los usuarios crear y utilizar solo las sesiones de cuadernos que estén asociadas a esos usuarios. Esta política también incluye otros permisos que AWS Glue necesita para gestionar los recursos de Glue en otros AWS servicios.

`AwsGlueSessionUserRestrictedNotebookServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedNotebookServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de abril de 2022 a las 15:27 UTC
- Hora de edición: 15 de agosto de 2024 a las 20:51 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AwsGlueSessionUserRestrictedPolicy

Descripción: proporciona permisos que permiten a los usuarios crear y utilizar únicamente las sesiones interactivas asociadas al usuario. Esta política también incluye permisos para que los usuarios puedan pasar expresamente un rol de sesión de Glue restringido.

`AwsGlueSessionUserRestrictedPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de abril de 2022 a las 21:31 UTC
- Hora de edición: 05 de agosto de 2024 a las 23:06 h UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AwsGlueSessionUserRestrictedServiceRole

Descripción: Proporciona acceso completo a todos los recursos de AWS Glue, excepto a las sesiones. Permite a los usuarios crear y utilizar solo las sesiones interactivas que están asociadas al usuario. Esta política también incluye otros permisos que AWS Glue necesita para gestionar los recursos de Glue en otros AWS servicios.

`AwsGlueSessionUserRestrictedServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AwsGlueSessionUserRestrictedServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de abril de 2022 a las 21:30 UTC
- Hora de edición: 05 de agosto de 2024 a las 23:14 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGrafanaAccountAdministrator

Descripción: proporciona acceso dentro de Amazon Grafana para crear y administrar espacios de trabajo para toda la organización.

`AWSGrafanaAccountAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGrafanaAccountAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de febrero de 2021 a las 00:20 UTC
- Hora de edición: 15 de febrero de 2022 a las 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGrafanaConsoleReadOnlyAccess

Descripción: acceso a operaciones de solo lectura en Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGrafanaConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de febrero de 2021 a las 00:10 UTC
- Hora de edición: 15 de febrero de 2022 a las 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGrafanaWorkspacePermissionManagement

Descripción: solo ofrece la posibilidad de actualizar los permisos de usuario y grupo para los espacios de trabajo de AWS Grafana.

`AWSGrafanaWorkspacePermissionManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGrafanaWorkspacePermissionManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 23 de febrero de 2021 a las 00:15 UTC
- Hora de edición: 15 de marzo de 2023 a las 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGrafanaWorkspacePermissionManagementV2

Descripción: proporciona la capacidad de actualizar los permisos de usuarios y grupos de IAM Identity Center (IdC) para los espacios de trabajo de Amazon Managed Grafana.

`AWSGrafanaWorkspacePermissionManagementV2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGrafanaWorkspacePermissionManagementV2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 05 de enero de 2024 a las 18:39 h UTC
- Hora de edición: 05 de enero de 2024 a las 18:39 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGreengrassFullAccess

Descripción: Esta política proporciona acceso completo a las acciones de configuración, administración e implementación de AWS Greengrass

`AWSGreengrassFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGreengrassFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de mayo de 2017 a las 00:47 UTC
- Hora de edición: 3 de mayo de 2017 a las 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGreengrassReadOnlyAccess

Descripción: Esta política proporciona acceso de solo lectura a las acciones de configuración, administración e implementación de AWS Greengrass

`AWSGreengrassReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGreengrassReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de octubre de 2018 a las 16:01 UTC
- Hora de edición: 30 de octubre de 2018 a las 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGreengrassResourceAccessRolePolicy

Descripción: Política para el rol de servicio de AWS Greengrass que permite el acceso a servicios relacionados, incluidos AWS Lambda e AWS IoT Things Shadow.

`AWSGreengrassResourceAccessRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGreengrassResourceAccessRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 14 de febrero de 2017 a las 21:17 UTC
- Hora de edición: 14 de noviembre de 2018 a las 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSGroundStationAgentInstancePolicy

Descripción: Proporciona a la instancia de punto final de Dataflow permisos para usar el AWS Ground Station Agent

`AWSGroundStationAgentInstancePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSGroundStationAgentInstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de marzo de 2023 a las 15:23 UTC
- Hora de edición: 29 de marzo de 2023 a las 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSHealth_EventProcessorServiceRolePolicy

Descripción: Permite a AWS Health activar la función de procesador de eventos de Health.

`AWSHealth_EventProcessorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de enero de 2023 a las 19:24 UTC
- Hora de edición: 13 de enero de 2023 a las 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSHealthFullAccess

Descripción: Permite el acceso completo a las API y notificaciones de AWS salud y al Personal Health Dashboard

`AWSHealthFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSHealthFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de diciembre de 2016 a las 12:30 UTC
- Hora de edición: 16 de noviembre de 2020 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSHealthImagingFullAccess

Descripción: Proporciona acceso completo al servicio AWS Health Imaging.

`AWSHealthImagingFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSHealthImagingFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de julio de 2023 a las 23:39 UTC
- Hora de edición: 25 de julio de 2023 a las 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSHealthImagingReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al servicio AWS Health Imaging.

`AWSHealthImagingReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSHealthImagingReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de julio de 2023 a las 23:40 UTC
- Hora de edición: 1 de agosto de 2023 a las 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIAMIdentityCenterAllowListForIdentityContext

Descripción: proporciona la lista de acciones que están permitidas para las funciones asumidas con el contexto de identidad del IAM Identity Center. AWS El Security Token Service (AWS STS) asocia automáticamente esta política a las funciones asumidas. El contexto de identidad se transmite como ProvidedContext.

`AWSIAMIdentityCenterAllowListForIdentityContext` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIAMIdentityCenterAllowListForIdentityContext` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de noviembre de 2023 a las 15:21 UTC
- Hora de edición: 01 de octubre de 2024 a las 14:19 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIdentitySyncFullAccess

Descripción: concede acceso completo al servicio Identity Sync

`AWSIdentitySyncFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIdentitySyncFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de marzo de 2022 a las 23:29 UTC
- Hora de edición: 23 de marzo de 2022 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIdentitySyncReadOnlyAccess

Descripción: acceso de solo lectura al servicio Identity Sync

`AWSIdentitySyncReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIdentitySyncReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de marzo de 2022 a las 23:29 UTC
- Hora de edición: 23 de marzo de 2022 a las 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSImageBuilderFullAccess

Descripción: Proporciona acceso completo a todas las acciones de AWS Image Builder y acceso limitado a los recursos a los AWS servicios relacionados.

`AWSImageBuilderFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSImageBuilderFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de diciembre de 2019 a las 18:25 UTC
- Hora de edición: 13 de abril de 2021 a las 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSImageBuilderReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a todas las acciones AWS de Image Builder.

`AWSImageBuilderReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSImageBuilderReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de diciembre de 2019 a las 22:29 UTC
- Hora de edición: 19 de diciembre de 2019 a las 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSImportExportFullAccess

Descripción: proporciona acceso de lectura y escritura a los trabajos creados bajo la Cuenta de AWS.

`AWSImportExportFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSImportExportFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSImportExportReadOnlyAccess

Descripción: proporciona acceso de solo lectura a los trabajos creados bajo la Cuenta de AWS.

`AWSImportExportReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSImportExportReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIncidentManagerIncidentAccessServiceRolePolicy

Descripción: Otorga al administrador de incidentes permisos para llamar a otros AWS servicios como parte de la gestión de un incidente.

`AWSIncidentManagerIncidentAccessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIncidentManagerIncidentAccessServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de noviembre de 2023 a las 00:01 UTC
- Hora de edición: 20 de febrero de 2024 a las 23:02 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIncidentManagerResolverAccess

Descripción: esta política concede permisos para iniciar, ver y actualizar incidentes con acceso completo a los eventos personalizados de la cronología, y a los elementos relacionados. Asigne esta política a los usuarios que crearán y resolverán los incidentes.

`AWSIncidentManagerResolverAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIncidentManagerResolverAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 10 de mayo de 2021 a las 06:12 UTC
- Hora de edición: 10 de mayo de 2021 a las 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIncidentManagerServiceRolePolicy

Descripción: esta política concede permiso al Administrador de incidentes para administrar los registros de incidentes y los recursos relacionados en su nombre.

`AWSIncidentManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de mayo de 2021 a las 03:34 UTC

- Hora editada: 28 de enero de 2025 a las 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoT1ClickFullAccess

Descripción: Proporciona acceso completo a AWS IoT 1-Click.

`AWSIoT1ClickFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoT1ClickFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2018 a las 22:10 UTC
- Hora de edición: 11 de mayo de 2018 a las 22:10 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoT1ClickReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoT1ClickReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de mayo de 2018 a las 21:49 UTC
- Hora de edición: 11 de mayo de 2018 a las 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTAnalyticsFullAccess

Descripción: proporciona acceso completo a IoT Analytics.

`AWSIoTAnalyticsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTAnalyticsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2018 a las 23:02 UTC
- Hora de edición: 18 de junio de 2018 a las 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTAnalyticsReadOnlyAccess

Descripción: proporciona acceso de solo lectura a IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTAnalyticsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2018 a las 21:37 UTC
- Hora de edición: 18 de junio de 2018 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTConfigAccess

Descripción: Esta política proporciona acceso completo a las acciones de configuración de AWS IoT

`AWSIoTConfigAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTConfigAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de octubre de 2015 a las 21:52 UTC
- Hora de edición: 27 de septiembre de 2019 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTConfigReadOnlyAccess

Descripción: Esta política proporciona acceso de solo lectura a las acciones de configuración de AWS IoT

`AWSIoTConfigReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTConfigReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de octubre de 2015 a las 21:52 UTC
- Hora de edición: 27 de septiembre de 2019 a las 20:52 UTC

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

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDataAccess

Descripción: Esta política brinda acceso completo a las acciones de mensajería de AWS IoT

`AWSIoTDataAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDataAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de octubre de 2015 a las 21:51 UTC
- Hora de edición: 23 de junio de 2021 a las 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Descripción: proporciona acceso de escritura a los grupos de objetos de IoT, así como acceso de lectura a los certificados de IoT para la ejecución de la acción de mitigación ADD_THINGS_TO_THING_GROUP

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:55 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderAudit

Descripción: proporciona acceso de lectura para IoT y recursos relacionados

`AWSIoTDeviceDefenderAudit` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderAudit` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 18 de julio de 2018 a las 21:17 UTC
- Hora de edición: 25 de noviembre de 2019 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Descripción: proporciona acceso para habilitar el registro de IoT para ejecutar la acción de mitigación ENABLE_IOT_LOGGING

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Descripción: proporciona a los mensajes acceso de publicación al tema de SNS para ejecutar la acción de mitigación PUBLISH_FINDING_TO_SNS

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Descripción: proporciona acceso de escritura a las políticas de IoT para ejecutar la acción de mitigación REPLACE_DEFAULT_POLICY_VERSION

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:04 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Descripción: proporciona acceso de escritura a los certificados de CA de IoT para ejecutar la acción de mitigación UPDATE_CA_CERTIFICATE

`AWSIoTDeviceDefenderUpdateCACertMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderUpdateCACertMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:05 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Descripción: proporciona acceso de escritura a los certificados de IoT para ejecutar la acción de mitigación UPDATE_DEVICE_CERTIFICATE

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de agosto de 2019 a las 17:06 UTC
- Hora de edición: 7 de agosto de 2019 a las 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceTesterForFreeRTOSFullAccess

Descripción: Permite que AWS IoT Device Tester ejecute el conjunto de calificaciones FreeRTOS al permitir el acceso a servicios como IoT, S3 e IAM

`AWSIoTDeviceTesterForFreeRTOSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceTesterForFreeRTOSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 12 de febrero de 2020 a las 20:33 UTC
- Hora de edición: 10 de agosto de 2023 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTDeviceTesterForGreengrassFullAccess

Descripción: Permite a AWS IoT Device Tester ejecutar el conjunto de calificaciones de AWS Greengrass al permitir el acceso a servicios relacionados, como Lambda, IoT, API Gateway e IAM

`AWSIoTDeviceTesterForGreengrassFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTDeviceTesterForGreengrassFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 20 de febrero de 2020 a las 21:21 UTC
- Hora de edición: 25 de junio de 2020 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTEventsFullAccess

Descripción: proporciona acceso completo a IoT Events.

`AWSIoTEventsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTEventsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 10 de enero de 2019 a las 22:51 UTC
- Hora de edición: 10 de enero de 2019 a las 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTEventsReadOnlyAccess

Descripción: proporciona acceso de solo lectura a IoT Events.

`AWSIoTEventsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTEventsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de enero de 2019 a las 22:50 UTC
- Hora de edición: 23 de septiembre de 2019 a las 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTFleetHubFederationAccess

Descripción: acceso federado para aplicaciones de IoT Fleet Hub

`AWSIoTFleetHubFederationAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTFleetHubFederationAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 15 de diciembre de 2020 a las 08:08 UTC
- Hora de edición: 4 de abril de 2022 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTFleetwiseServiceRolePolicy

Descripción: Otorga permisos a AWS los recursos y metadatos utilizados o administrados AWSIo TFleetwise por las funciones auxiliares

`AWSIoTFleetwiseServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de septiembre de 2022 a las 23:27 UTC
- Hora de edición: 21 de septiembre de 2022 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTFullAccess

Descripción: Esta política proporciona acceso completo a las acciones de configuración y mensajería de AWS IoT

`AWSIoTFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de octubre de 2015 a las 15:19 UTC
- Hora de edición: 19 de mayo de 2022 a las 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTLogging

Descripción: Permite la creación de grupos de Amazon CloudWatch Log y la transmisión de registros a los grupos

`AWSIoTLogging` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTLogging` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de octubre de 2015 a las 15:17 UTC
- Hora de edición: 8 de octubre de 2015 a las 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTManagedIntegrationsFullAccess

Descripción: Proporciona acceso completo a las integraciones gestionadas para AWS IoT Device Management y servicios relacionados.

`AWSIoTManagedIntegrationsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTManagedIntegrationsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de marzo de 2025 a las 19:22 UTC
- Hora editada: 5 de marzo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTManagedIntegrationsRolePolicy

Descripción: Proporciona a las integraciones gestionadas el permiso de AWS IoT Device Management para publicar registros y métricas en su nombre.

`AWSIoTManagedIntegrationsRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de marzo de 2025 a las 21:22 UTC
- Hora editada: 5 de marzo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTOTAUpdate

Descripción: Permite acceder para crear un trabajo de AWS IoT y describir el trabajo del firmante de AWS código

`AWSIoTOTAUpdate` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTOTAUpdate` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de diciembre de 2017 a las 20:36 UTC
- Hora de edición: 20 de diciembre de 2017 a las 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIotRoboRunnerFullAccess

Descripción: Esta política otorga permisos que permiten el acceso total a AWS Iot RoboRunner.

`AWSIotRoboRunnerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIotRoboRunnerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2021 a las 03:54 UTC
- Hora de edición: 23 de febrero de 2023 a las 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIotRoboRunnerReadOnly

Descripción: Esta política otorga permisos que permiten el acceso de solo lectura a AWS la IoT. RoboRunner

`AWSIotRoboRunnerReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIotRoboRunnerReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2021 a las 03:43 UTC
- Hora de edición: 16 de noviembre de 2022 a las 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIotRoboRunnerServiceRolePolicy

Descripción: Permite que el AWS IoT RoboRunner gestione AWS los recursos asociados en nombre del cliente.

`AWSIotRoboRunnerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de febrero de 2023 a las 16:56 UTC
- Hora de edición: 21 de febrero de 2023 a las 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTRuleActions

Descripción: Permite el acceso a todos los AWS servicios compatibles con las acciones de reglas de AWS IoT

`AWSIoTRuleActions` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTRuleActions` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 8 de octubre de 2015 a las 15:14 UTC
- Hora de edición: 16 de enero de 2018 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTSiteWiseConsoleFullAccess

Descripción: Proporciona acceso completo para administrar el AWS IoT SiteWise mediante AWS Management Console. Tenga en cuenta que esta política también permite crear y enumerar los almacenes de datos que se utilizan con la AWS IoT SiteWise (por ejemplo, AWS IoT Analytics), acceder a la lista y visualización de los recursos de AWS IoT Greengrass, enumerar y modificar AWS los secretos de Secrets Manager, recuperar sombras ocultas de AWS IoT, enumerar recursos con etiquetas específicas y crear y utilizar un rol vinculado a un servicio para la IoT. AWS SiteWise

`AWSIoTSiteWiseConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTSiteWiseConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 31 de mayo de 2019 a las 21:37 UTC
- Hora de edición: 31 de mayo de 2019 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTSiteWiseFullAccess

Descripción: Proporciona acceso completo a IoT SiteWise.

`AWSIoTSiteWiseFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTSiteWiseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de diciembre de 2018 a las 20:53 UTC
- Hora de edición: 4 de diciembre de 2018 a las 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTSiteWiseMonitorPortalAccess

Descripción: Esta política otorga permisos para acceder a los SiteWise activos y datos de activos de AWS IoT, crear recursos de AWS IoT SiteWise Monitor y enumerar los usuarios de AWS SSO.

`AWSIoTSiteWiseMonitorPortalAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTSiteWiseMonitorPortalAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 19 de mayo de 2020 a las 20:01 UTC
- Hora de edición: 19 de mayo de 2020 a las 20:01 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTSiteWiseMonitorServiceRolePolicy

Descripción: Esta función otorga permisos de SiteWise monitoreo de AWS IoT para acceder a sus SiteWise activos y propiedades de activos de AWS IoT y crear proyectos, paneles y políticas de acceso de AWS IoT Sitewise a través de portales de AWS IoT SiteWise .

`AWSIoTSiteWiseMonitorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2019 a las 00:59 UTC
- Hora de edición: 13 de diciembre de 2019 a las 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTSiteWiseReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTSiteWiseReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de diciembre de 2018 a las 20:55 UTC
- Hora de edición: 16 de septiembre de 2022 a las 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTThingsRegistration

Descripción: Esta política permite a los usuarios registrar cosas de forma masiva mediante la StartThingRegistrationTask API de AWS IoT

`AWSIoTThingsRegistration` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTThingsRegistration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2017 a las 20:21 UTC
- Hora de edición: 5 de octubre de 2020 a las 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTTwinMakerServiceRolePolicy

Descripción: Permite que el AWS IoT llame TwinMaker a otros AWS servicios y sincronice sus recursos en su nombre.

`AWSIoTTwinMakerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de noviembre de 2023 a las 18:59 UTC
- Hora de edición: 13 de noviembre de 2023 a las 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessDataAccess

Descripción: Permite el acceso de los datos de identidad asociados a los dispositivos AWS IoT Wireless.

`AWSIoTWirelessDataAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessDataAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:31 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessFullAccess

Descripción: Permite a la identidad asociada el acceso total a todas las operaciones de AWS IoT Wireless.

`AWSIoTWirelessFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:27 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessFullPublishAccess

Descripción: proporciona a IoT Wireless acceso total para publicar en IoT Rules Engine en su nombre.

`AWSIoTWirelessFullPublishAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessFullPublishAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:29 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessGatewayCertManager

Descripción: permite a la identidad asociada obtener acceso para crear, enumerar y describir certificados de IoT

`AWSIoTWirelessGatewayCertManager` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessGatewayCertManager` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:30 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessLogging

Descripción: Permite que la identidad asociada cree grupos de Amazon CloudWatch Logs y transmita registros a los grupos.

`AWSIoTWirelessLogging` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessLogging` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:32 UTC

- Hora de edición: 15 de diciembre de 2020 a las 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIoTWirelessReadOnlyAccess

Descripción: Permite el acceso de solo lectura de la identidad asociada a la tecnología inalámbrica AWS IoT.

`AWSIoTWirelessReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIoTWirelessReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de diciembre de 2020 a las 15:28 UTC
- Hora de edición: 15 de diciembre de 2020 a las 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIPAMServiceRolePolicy

Descripción: Permite que VPC IP Address Manager acceda a los recursos de VPC y se integre con Organizations en su nombre AWS .

`AWSIPAMServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2021 a las 19:08 UTC
- Hora editada: 8 de noviembre de 2024 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIQContractServiceRolePolicy

Descripción: Utilizado por AWS IQ para ejecutar solicitudes de pago en nombre de un cliente

`AWSIQContractServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de agosto de 2019 a las 19:28 UTC
- Hora de edición: 22 de agosto de 2019 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIQFullAccess

Descripción: Proporciona acceso completo a AWS IQ

`AWSIQFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSIQFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 4 de abril de 2019 a las 23:13 UTC
- Hora de edición: 25 de septiembre de 2019 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSIQPermissionServiceRolePolicy

Descripción: Permite a AWS IQ gestionar el papel que asumen los expertos en AWS IQ.

`AWSIQPermissionServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de agosto de 2019 a las 19:36 UTC
- Hora de edición: 22 de agosto de 2019 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Descripción: Permite el acceso a AWS los servicios y recursos necesarios para los almacenes de claves personalizadas de AWS KMS

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 20:10 UTC
- Hora de edición: 10 de noviembre de 2023 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Descripción: Permite a AWS KMS sincronizar las propiedades compartidas de las claves multirregionales.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de junio de 2021 a las 15:37 UTC
- Hora editada: 13 de noviembre de 2024 a las 22:53 UTC

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

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSKeyManagementServicePowerUser

Descripción: Proporciona acceso al Servicio de administración de AWS claves (KMS).

`AWSKeyManagementServicePowerUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSKeyManagementServicePowerUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 7 de marzo de 2017 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLakeFormationCrossAccountManager

Descripción: proporciona acceso entre cuentas a los recursos de Glue a través de Lake Formation. También, otorga acceso de lectura a otros servicios necesarios, como las organizaciones y el administrador de acceso a los recursos

`AWSLakeFormationCrossAccountManager` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLakeFormationCrossAccountManager` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de agosto de 2020 a las 20:59 UTC
- Hora editada: 25 de febrero de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLakeFormationDataAdmin

Descripción: Otorga acceso administrativo a AWS Lake Formation y servicios relacionados, como AWS Glue, para gestionar los lagos de datos

`AWSLakeFormationDataAdmin` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLakeFormationDataAdmin` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de agosto de 2019 a las 17:33 UTC
- Hora editada: 3 de diciembre de 2024 a las 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambda_FullAccess

Descripción: Otorga acceso completo al servicio AWS Lambda, a las funciones de la consola AWS Lambda y a otros servicios relacionados. AWS

`AWSLambda_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambda_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS

- Hora de creación: 17 de noviembre de 2020 a las 21:14 UTC
- Hora editada: 17 de marzo de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambda_ReadOnlyAccess

Descripción: Otorga acceso de solo lectura al AWS servicio Lambda, a las funciones de la consola AWS Lambda y a otros servicios relacionados. AWS

`AWSLambda_ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambda_ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 17 de noviembre de 2020 a las 21:10 UTC
- Hora editada: 17 de marzo de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaBasicExecutionRole

Descripción: Proporciona permisos de escritura a CloudWatch los registros.

`AWSLambdaBasicExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaBasicExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:03 UTC
- Hora de edición: 9 de abril de 2015 a las 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaDynamoDBExecutionRole

Descripción: Proporciona acceso de lista y lectura a las transmisiones de DynamoDB y permisos de escritura en los registros. CloudWatch

`AWSLambdaDynamoDBExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaDynamoDBExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:09 UTC
- Hora de edición: 9 de abril de 2015 a las 15:09 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaENIManagementAccess

Descripción: Proporciona los permisos mínimos para que una función Lambda administre ENIs (cree, describa, elimine) utilizada por una función Lambda habilitada para VPC.

`AWSLambdaENIManagementAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaENIManagementAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de diciembre de 2016 a las 00:37 UTC
- Hora de edición: 1 de octubre de 2020 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
```

```
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaExecute

Descripción: Proporciona Put, Get acceso a S3 y acceso completo a CloudWatch los registros.

`AWSLambdaExecute` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaExecute` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:::*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaFullAccess

Descripción: esta política está en proceso de quedar obsoleta. Consulte la documentación para obtener orientación: https://docs.aws.amazon.com/lambda/ latest/dg/access - control-identity-based .html. Proporciona acceso completo a Lambda, S3, DynamoDB, Metrics and Logs. CloudWatch

`AWSLambdaFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2017 a las 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaInvocation-DynamoDB

Descripción: proporciona acceso de lectura a DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaInvocation-DynamoDB` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaKinesisExecutionRole

Descripción: Proporciona acceso de lista y lectura a las transmisiones de Kinesis y permisos de escritura en los CloudWatch registros.

`AWSLambdaKinesisExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaKinesisExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de abril de 2015 a las 15:14 UTC
- Hora de edición: 19 de noviembre de 2018 a las 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaMSKExecutionRole

Descripción: Proporciona los permisos necesarios para acceder al clúster de MSK dentro de una VPC, ENIs administrar (crear, describir, eliminar) en la VPC y escribir permisos en los registros. CloudWatch

`AWSLambdaMSKExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaMSKExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2020 a las 17:35 UTC

- Hora de edición: 2 de agosto de 2022 a las 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaReplicator

Descripción: concede a Lambda Replicator los permisos necesarios para replicar funciones en las regiones

`AWSLambdaReplicator` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de mayo de 2017 a la 17:53 UTC
- Hora de edición: 8 de diciembre de 2017 a las 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaRole

Descripción: Política predeterminada para el rol de servicio de AWS Lambda.

`AWSLambdaRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaSQSQueueExecutionRole

Descripción: Proporciona acceso a los atributos de recepción, eliminación de mensajes y lectura a las colas de SQS y permisos de escritura en los CloudWatch registros.

`AWSLambdaSQSQueueExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaSQSQueueExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de junio de 2018 a las 21:50 UTC
- Hora de edición: 14 de junio de 2018 a las 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLambdaVPCAccessExecutionRole

Descripción: Proporciona permisos mínimos para que una función de Lambda se ejecute mientras se accede a un recurso dentro de una VPC: crear, describir, eliminar interfaces de red y permisos de escritura en los registros. CloudWatch

`AWSLambdaVPCAccessExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLambdaVPCAccessExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de febrero de 2016 a las 23:15 UTC
- Hora de edición: 05 de enero de 2024 a las 22:38 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerConsumptionPolicy

Descripción: Proporciona permisos para permitir el acceso a las acciones de la API AWS License Manager que se deben consumir con las licencias a las que el usuario tiene derechos.

`AWSLicenseManagerConsumptionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSLicenseManagerConsumptionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2021 a las 23:18 UTC
- Hora de edición: 11 de agosto de 2021 a las 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Descripción: Permite que AWS License Manager Linux Subscriptions Service gestione los recursos en su nombre.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de diciembre de 2022 a las 18:54 UTC
- Hora de edición: 08 de julio de 2024 a las 22:04 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerMasterAccountRolePolicy

Descripción: Política de funciones de la cuenta maestra del servicio AWS License Manager

`AWSLicenseManagerMasterAccountRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:03 UTC
- Hora de edición: 31 de mayo de 2022 a las 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerMemberAccountRolePolicy

Descripción: Política de roles de cuentas de miembros del servicio AWS License Manager

`AWSLicenseManagerMemberAccountRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:04 UTC
- Hora de edición: 15 de noviembre de 2019 a las 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerServiceRolePolicy

Descripción: Política de funciones predeterminadas del servicio AWS License Manager

`AWSLicenseManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:02 UTC
- Hora de edición: 30 de julio de 2021 a las 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "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" : [
        "*"
      ]
    }
```

```
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Descripción: Permite que el Servicio de Suscripciones de Usuarios de AWS License Manager administre los recursos en su nombre.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de julio de 2022 a las 01:17 UTC
- Hora editada: 8 de noviembre de 2024 a las 02:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "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"
          ]
        }
      },
      "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" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSM2ServicePolicy

Descripción: Permite que AWS M2 administre AWS los recursos en su nombre.

`AWSM2ServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de junio de 2022 a las 20:26 UTC
- Hora de edición: 7 de junio de 2022 a las 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSManagedServices_ContactsServiceRolePolicy

Descripción: Permite a AWS Managed Services leer los valores de las etiquetas de los AWS recursos

`AWSManagedServices_ContactsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de marzo de 2023 a las 17:07 UTC
- Hora de edición: 23 de marzo de 2023 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Descripción: AWS Managed Services: política para gestionar la infraestructura de controles de detección

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de diciembre de 2022 a las 23:11 UTC
- Hora de edición: 19 de diciembre de 2022 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSManagedServices_EventsServiceRolePolicy

Descripción: Política de AWS Managed Services para habilitar la función de procesador de eventos AMS.

`AWSManagedServices_EventsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de febrero de 2023 a las 18:41 UTC
- Hora de edición: 7 de febrero de 2023 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Descripción: Permite que la función de informes de autoservicio del Servicio AWS gestionado de Amazon lea los datos de AWS la organización en tu nombre para permitir la elaboración de informes agregados a nivel de organización

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 8 de enero de 2025 a las 21:22 UTC
- Hora editada: 8 de enero de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSManagedServicesDeploymentToolkitPolicy

Descripción: Permite a AWS Managed Services gestionar el kit de herramientas de implementación en su nombre.

`AWSManagedServicesDeploymentToolkitPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de junio de 2022 a las 18:33 UTC
- Hora de edición: 04 de abril de 2024 a las 20:41 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceAmiIngestion

Descripción: Permite AWS Marketplace copiar tus imágenes de Amazon Machine (AMIs) para incluirlas en AWS Marketplace

`AWSMarketplaceAmiIngestion` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceAmiIngestion` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de septiembre de 2020 a las 20:55 UTC
- Hora de edición: 25 de septiembre de 2020 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceDeploymentServiceRolePolicy

Descripción: Permite AWS Marketplace crear y gestionar los parámetros de despliegue de vendedores para los productos a los que te suscribes AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2023 a las 23:34 UTC
- Hora de edición: 15 de noviembre de 2023 a las 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
```

```
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceFullAccess

Descripción: Ofrece la posibilidad de suscribirse y cancelar la suscripción al AWS Marketplace software, permite a los usuarios gestionar las instancias de software de Marketplace desde la página «Su software» de Marketplace y proporciona acceso administrativo a. EC2

`AWSMarketplaceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 11 de febrero de 2015 a las 17:21 UTC
- Hora editada: 7 de mayo de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceGetEntitlements

Descripción: Proporciona acceso de lectura a los AWS Marketplace derechos

`AWSMarketplaceGetEntitlements` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceGetEntitlements` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 27 de marzo de 2017 a las 19:37 UTC
- Hora de edición: 05 de abril de 2024 a las 01:27 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceImageBuildFullAccess

Descripción: Proporciona acceso completo a la función de creación de imágenes AWS Marketplace privadas. Además de crear imágenes privadas, también concede permisos para añadir etiquetas a las imágenes, y lanzar y finalizar instancias ec2.

`AWSMarketplaceImageBuildFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceImageBuildFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 31 de julio de 2018 a las 23:29 UTC
- Hora de edición: 4 de marzo de 2022 a las 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceLicenseManagementServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o gestionados por ellos AWS Marketplace para la administración de licencias.

`AWSMarketplaceLicenseManagementServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2020 a las 08:33 UTC
- Hora de edición: 3 de diciembre de 2020 a las 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceManageSubscriptions

Descripción: Ofrece la posibilidad de suscribirse y cancelar la suscripción al AWS Marketplace software

`AWSMarketplaceManageSubscriptions` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceManageSubscriptions` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 20 de noviembre de 2024 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceMeteringFullAccess

Descripción: Proporciona acceso completo a AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceMeteringFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de marzo de 2016 a las 22:39 UTC
- Hora de edición: 17 de marzo de 2016 a las 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceMeteringRegisterUsage

Descripción: Proporciona permisos para registrar un recurso y realizar un seguimiento del uso a través del servicio de AWS Marketplace medición.

`AWSMarketplaceMeteringRegisterUsage` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceMeteringRegisterUsage` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de noviembre de 2019 a las 01:17 UTC
- Hora de edición: 21 de noviembre de 2019 a las 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceProcurementSystemAdminFullAccess

Descripción: Proporciona acceso completo a todas las acciones administrativas para la integración de la AWS Marketplace contratación electrónica.

`AWSMarketplaceProcurementSystemAdminFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceProcurementSystemAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de junio de 2019 a las 13:07 UTC
- Hora de edición: 25 de junio de 2019 a las 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplacePurchaseOrdersServiceRolePolicy

Descripción: Permite el acceso de los AWS Marketplace servicios a la gestión de pedidos de compra.

`AWSMarketplacePurchaseOrdersServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de octubre de 2021 a las 15:12 UTC
- Hora de edición: 27 de octubre de 2021 a las 15:12 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceRead-only

Descripción: Ofrece la posibilidad de revisar AWS Marketplace las suscripciones

`AWSMarketplaceRead-only` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceRead-only` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 7 de mayo de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o gestionados por ellos AWS Marketplace para la autorización de reventa.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 05 de marzo de 2024 a las 18:47 h UTC
- Hora de edición: 05 de marzo de 2024 a las 18:47 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:AWSMarketplace/
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" : "AllowResaleAuthorizationShareActionsRAMAccept",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "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"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceSellerFullAccess

Descripción: proporciona acceso completo a todas las operaciones del vendedor en el AWS Marketplace y otros AWS servicios, como la gestión de AMI.

`AWSMarketplaceSellerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceSellerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de julio de 2019 a las 20:40 UTC
- Hora editada: 14 de enero de 2025 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Versión de la política

Versión de la política: v16 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    },
    {
      "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"
      ],
      "Resource" : "*"
    },
    {
      "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/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceSellerOfferManagement

Descripción: Proporciona a los vendedores acceso a las actividades de gestión de ofertas y acuerdos.

`AWSMarketplaceSellerOfferManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceSellerOfferManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de noviembre de 2024 a las 00:41 UTC
- Hora editada: 19 de noviembre de 2024 a las 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
```

```
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceSellerProductsFullAccess

Descripción: proporciona a los vendedores acceso completo a la página AWS Marketplace de productos de gestión y a otros AWS servicios, como la gestión de AMI.

`AWSMarketplaceSellerProductsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceSellerProductsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de julio de 2019 a las 21:06 UTC
- Hora editada: 10 de diciembre de 2024 a las 19:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMarketplaceSellerProductsReadOnly

Descripción: proporciona a los vendedores acceso de solo lectura a la página AWS Marketplace de productos de gestión.

`AWSMarketplaceSellerProductsReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMarketplaceSellerProductsReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 2 de julio de 2019 a las 21:40 UTC
- Hora editada: 10 de diciembre de 2024 a las 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMediaConnectServicePolicy

Descripción: la política predeterminada que permite el acceso a Servicios de AWS los recursos utilizados o gestionados por ellos MediaConnect.

`AWSMediaConnectServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de abril de 2023 a las 22:11 UTC
- Hora de edición: 3 de abril de 2023 a las 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMediaLiveAnywhereServiceRolePolicy

Descripción: Permite a MediaLive Anywhere crear y gestionar AWS recursos en su nombre.

`AWSMediaLiveAnywhereServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de abril de 2025 a las 22:07 UTC
- Hora editada: 14 de abril de 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMediaTailorServiceRolePolicy

Descripción: Habilitar el acceso a AWS los recursos utilizados o administrados por MediaTailor

`AWSMediaTailorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de septiembre de 2021 a las 22:27 UTC
- Hora de edición: 17 de septiembre de 2021 a las 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubDiscoveryAccess

Descripción: La política AWSMigration HubService permite llamar AWSApplication DiscoveryService en nombre del cliente.

`AWSMigrationHubDiscoveryAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubDiscoveryAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:30 UTC
- Hora de edición: 6 de agosto de 2020 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubDMSAccess

Descripción: política para que Database Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

`AWSMigrationHubDMSAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubDMSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 14:00 UTC
- Hora de edición: 7 de octubre de 2019 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubFullAccess

Descripción: política administrada para proporcionar al cliente acceso a Migration Hub Service

`AWSMigrationHubFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de agosto de 2017 a las 14:02 UTC
- Hora de edición: 19 de junio de 2019 a las 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubOrchestratorConsoleFullAccess

Descripción: Ofrece acceso limitado a AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service y AWS Secrets Manager. Esta política también otorga acceso completo al servicio AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubOrchestratorConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de abril de 2022 a las 02:26 UTC

- Hora de edición: 05 de diciembre de 2023 a las 17:34 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubOrchestratorInstanceRolePolicy

Descripción: Esta política debe adjuntarse a las instancias migradas de SAP y MGN para que nuestro servicio pueda organizar las instancias mediante la descarga de scripts de S3 y obtener los valores secretos de la instancia. EC2

`AWSMigrationHubOrchestratorInstanceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubOrchestratorInstanceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 20 de abril de 2022 a las 02:43 UTC

- Hora de edición: 20 de abril de 2022 a las 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubOrchestratorPlugin

Descripción: Proporciona acceso limitado a Amazon Simple Storage Service, AWS Secrets Manager y acciones relacionadas con complementos para AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubOrchestratorPlugin` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de abril de 2022 a las 02:25 UTC
- Hora de edición: 20 de abril de 2022 a las 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubOrchestratorServiceRolePolicy

Descripción: proporciona los permisos necesarios para que el Orquestador de Migration Hub migre y modernice las cargas de trabajo en las instalaciones

`AWSMigrationHubOrchestratorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de abril de 2022 a las 02:24 UTC
- Hora de edición: 04 de marzo de 2024 a las 18:25 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Descripción: Otorga acceso completo a los espacios de refactorización de AWS Migration Hub y otros servicios AWS relacionados, excepto AWS Transit Gateway y los grupos de EC2 seguridad que no son necesarios cuando se utilizan entornos sin un puente de red. Esta política también excluye

los permisos necesarios para AWS Lambda AWS y Resource Access Manager, ya que su alcance se puede reducir en función de las etiquetas.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 3 de abril de 2023 a las 20:09 UTC
- Hora de edición: 11 de abril de 2024 a las 18:16 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Descripción: Utilícela en el rol de servicio de IAM transferido al documento de automatización de SSM AWSRefactorSpaces-CreateResources para conceder los permisos necesarios para ejecutar la automatización. La política otorga acceso de lectura y escritura a las EC2 etiquetas para realizar un seguimiento del progreso de la automatización. Cuando el puente de red del entorno de Refactor Spaces está habilitado, la automatización también agrega el grupo de seguridad del entorno a la EC2 instancia para permitir el tráfico desde otros servicios de Refactor Spaces del entorno. A su vez, la política permite el acceso a los parámetros SSM de las acciones posteriores al lanzamiento del Servicio de migración de aplicaciones.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 10 de agosto de 2023 a las 15:08 UTC
- Hora de edición: 10 de agosto de 2023 a las 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-
*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubRefactorSpacesFullAccess

Descripción: Otorga acceso completo a AWS MigrationHub Refactor Spaces, a las funciones de la consola de AWS MigrationHub Refactor Spaces y a otros AWS servicios relacionados, excepto los permisos necesarios para AWS Lambda y AWS Resource Access Manager, ya que su alcance se puede reducir en función de las etiquetas.

`AWSMigrationHubRefactorSpacesFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubRefactorSpacesFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2021 a las 07:12 UTC
- Hora de edición: 11 de abril de 2024 a las 17:45 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubRefactorSpacesServiceRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por AWS Migration Hub Refactor Spaces.

`AWSMigrationHubRefactorSpacesServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2021 a las 06:50 UTC
- Hora de edición: 20 de julio de 2023 a las 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubSMSAccess

Descripción: política para que Server Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

`AWSMigrationHubSMSAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubSMSAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de agosto de 2017 a las 13:57 UTC
- Hora de edición: 7 de octubre de 2019 a las 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubStrategyCollector

Descripción: Otorga permisos para permitir la comunicación con el servicio de recomendaciones estratégicas de AWS Migration Hub, el acceso de lectura y escritura a los buckets de S3

relacionados con el servicio, el acceso a Amazon API Gateway para cargar registros y métricas, el acceso de AWS Secrets AWS Manager para obtener credenciales y cualquier servicio relacionado.

`AWSMigrationHubStrategyCollector` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubStrategyCollector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de octubre de 2021 a las 20:15 UTC
- Hora de edición: 01 de abril de 2024 a las 16:21 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubStrategyConsoleFullAccess

Descripción: Otorga acceso completo al servicio de recomendaciones estratégicas de AWS Migration Hub y acceso a AWS los servicios relacionados a través del AWS Management Console.

`AWSMigrationHubStrategyConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMigrationHubStrategyConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de octubre de 2021 a las 20:13 UTC
- Hora de edición: 9 de noviembre de 2022 a las 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMigrationHubStrategyServiceRolePolicy

Descripción: Habilite el acceso a AWS los recursos utilizados o administrados por el servicio de recomendaciones estratégicas de AWS Migration Hub.

`AWSMigrationHubStrategyServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de octubre de 2021 a las 20:02 UTC
- Hora de edición: 19 de octubre de 2021 a las 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMobileHub_FullAccess

Descripción: Esta política se puede adjuntar a cualquier usuario, rol o grupo para conceder a los usuarios permiso para crear, eliminar y modificar proyectos (y sus AWS recursos asociados) en AWS Mobile Hub. También, incluye permisos para generar y descargar ejemplos de código fuente de aplicaciones móviles, para cada proyecto de Mobile Hub.

`AWSMobileHub_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMobileHub_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de enero de 2016 a las 19:56 UTC
- Hora de edición: 19 de diciembre de 2019 a las 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMobileHub_ReadOnly

Descripción: Esta política se puede adjuntar a cualquier usuario, función o grupo para conceder a los usuarios permiso para publicar y ver proyectos en AWS Mobile Hub. También, incluye permisos

para generar y descargar ejemplos de código fuente de aplicaciones móviles, para cada proyecto de Mobile Hub. No permite al usuario modificar configuraciones de los proyectos de Mobile Hub.

`AWSMobileHub_ReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMobileHub_ReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 5 de enero de 2016 a las 19:55 UTC
- Hora de edición: 23 de julio de 2018 a las 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSMSKReplicatorExecutionRole

Descripción: concede permisos al Replicador Amazon MSK para replicar datos entre los clústeres de MSK.

`AWSMSKReplicatorExecutionRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSMSKReplicatorExecutionRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 06 de diciembre de 2023 a las 00:07 h UTC
- Hora de edición: 25 de marzo de 2024 a las 21:36 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkFirewallFullAccess

Descripción: Otorga acceso completo al servicio AWS Network Firewall, incluidos los permisos para crear, configurar, administrar y eliminar recursos, políticas y grupos de reglas del firewall. Además, incluye permisos para modificar los puntos de conexión de la VPC, las políticas de bucket de S3, las configuraciones de CloudWatch registros y la creación de funciones vinculadas a servicios para los servicios de Network Firewall y entrega de registros

`AWSNetworkFirewallFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSNetworkFirewallFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 10 de junio de 2025 a las 21:52 UTC
- Hora editada: 10 de junio de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkFirewallReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los recursos de AWS Network Firewall a través de la AWS Management Console CLI y. SDKs Esta política permite a los usuarios ver y supervisar las configuraciones, las políticas, los grupos de reglas y los recursos asociados del firewall, sin la posibilidad de realizar cambios.

`AWSNetworkFirewallReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSNetworkFirewallReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de junio de 2025 a las 21:52 UTC
- Hora editada: 10 de junio de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "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"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkFirewallServiceRolePolicy

Descripción: Permita que AWSNetwork Firewall cree y administre los recursos necesarios para sus firewalls.

`AWSNetworkFirewallServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2020 a las 17:17 UTC
- Hora de edición: 30 de marzo de 2023 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkManagerCloudWANServiceRolePolicy

Descripción: Permitir NetworkManager el acceso a los recursos asociados a su red principal

`AWSNetworkManagerCloudWANServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de julio de 2022 a las 12:17 UTC
- Hora de edición: 12 de julio de 2022 a las 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkManagerFullAccess

Descripción: Proporciona acceso completo a Amazon NetworkManager a través de AWS Management Console.

`AWSNetworkManagerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSNetworkManagerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 17:37 UTC
- Hora de edición: 3 de diciembre de 2019 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkManagerReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon NetworkManager a través del AWS Management Console.

`AWSNetworkManagerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSNetworkManagerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2019 a las 17:35 UTC
- Hora de edición: 3 de diciembre de 2019 a las 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSNetworkManagerServiceRolePolicy

Descripción: Permitir NetworkManager el acceso a los recursos asociados a sus redes globales

`AWSNetworkManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 14:03 UTC
- Hora de edición: 27 de julio de 2022 a las 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSObservabilityAdminServiceRolePolicy

Descripción: Proporciona acceso para administrar AWS Config Configuration Recorder, administrar el AWS Config Configuration Aggregator, crear un AWS rol vinculado al servicio de configuración para la funcionalidad de Configuration Recorder, consumir los datos de configuración del grabador y leer los datos de la organización para AWS las funciones organizativas.

`AWSObservabilityAdminServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 27 de noviembre de 2024 a las 19:36 UTC
- Hora editada: 27 de noviembre de 2024 a las 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorks_FullAccess

Descripción: Proporciona acceso completo a AWS OpsWorks.

`AWSOpsWorks_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorks_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de enero de 2021 a las 16:29 UTC
- Hora de edición: 22 de enero de 2021 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "opsworks.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksCloudWatchLogs

Descripción: Permite que OpsWorks las instancias con la CWLogs integración habilitada envíen registros y creen los grupos de registros necesarios

`AWSOpsWorksCloudWatchLogs` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksCloudWatchLogs` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de marzo de 2017 a las 17:47 UTC
- Hora de edición: 30 de marzo de 2017 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksCMInstanceProfileRole

Descripción: Proporciona acceso a S3 para las instancias lanzadas por OpsWorks CM.

`AWSOpsWorksCMInstanceProfileRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksCMInstanceProfileRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de noviembre de 2016 a las 09:48 UTC
- Hora de edición: 23 de abril de 2021 a las 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:SignalResource"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
      "Effect" : "Allow"
    },
    {
      "Action" : "acm:GetCertificate",
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Effect" : "Allow"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksCMServiceRole

Descripción: Política de roles de servicio que se utilizará para crear servidores OpsWorks CM.

`AWSOpsWorksCMServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksCMServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de noviembre de 2016 a las 09:49 UTC
- Hora de edición: 23 de abril de 2021 a las 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "tag:UntagResources",
        "tag:TagResources"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ssm:*::document/*",
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
```

```
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RunInstances",
        "ec2:StopInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:opsworks-cm:*:*:server/*"
      ],
      "Action" : [
        "opsworks-cm:DeleteServer",
        "opsworks-cm:StartMaintenance"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
      ],
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-opsworks-cm-*",
        "arn:aws:iam::*:role/service-role/aws-opsworks-cm-*"
      ],
      "Action" : [
        "iam:PassRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "acm:DeleteCertificate",
        "acm:ImportCertificate"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksInstanceRegistration

Descripción: proporciona acceso para que una EC2 instancia de Amazon se registre en una AWS OpsWorks pila.

`AWSOpsWorksInstanceRegistration` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksInstanceRegistration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de junio de 2016 a las 14:23 UTC
- Hora de edición: 3 de junio de 2016 a las 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksRegisterCLI_EC2

Descripción: Política para permitir el registro de EC2 instancias mediante la OpsWorks CLI

`AWSOpsWorksRegisterCLI_EC2` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksRegisterCLI_EC2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2019 a las 15:56 UTC
- Hora de edición: 18 de junio de 2019 a las 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOpsWorksRegisterCLI_OnPremises

Descripción: Política para permitir el registro de instancias locales a través de la CLI OpsWorks

`AWSOpsWorksRegisterCLI_OnPremises` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOpsWorksRegisterCLI_OnPremises` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2019 a las 15:33 UTC
- Hora de edición: 18 de junio de 2019 a las 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateUser",
        "iam:CreateAccessKey"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOrganizationsFullAccess

Descripción: Proporciona acceso completo a AWS Organizations.

`AWSOrganizationsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOrganizationsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de noviembre de 2018 a las 20:31 UTC
- Hora editada: 22 de abril de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOrganizationsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Organizations AWS .

`AWSOrganizationsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOrganizationsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de noviembre de 2018 a las 20:32 UTC
- Hora de edición: 07 de junio de 2024 a las 21:32 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOrganizationsServiceTrustPolicy

Descripción: Una política que permite a AWS las Organizaciones compartir la confianza con otras, aprobada con el Servicios de AWS fin de simplificar la configuración del cliente.

`AWSOrganizationsServiceTrustPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de octubre de 2017 a las 23:04 UTC
- Hora de edición: 1 de noviembre de 2017 a las 06:01 UTC

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

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOutpostsAuthorizeServerPolicy

Descripción: esta política concede permisos que permiten instalar un servidor Outpost en la red en las instalaciones.

`AWSOutpostsAuthorizeServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSOutpostsAuthorizeServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de enero de 2023 a las 19:23 UTC
- Hora de edición: 4 de enero de 2023 a las 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSOutpostsServiceRolePolicy

Descripción: Política de roles vinculados al servicio para permitir el acceso a AWS los recursos gestionados por AWS Outposts

`AWSOutpostsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2020 a las 22:55 UTC
- Hora editada: 17 de abril de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaApplianceRolePolicy

Descripción: Permite que el software de AWS IoT de un dispositivo AWS Panorama cargue registros en Amazon CloudWatch.

`AWSPanoramaApplianceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaApplianceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:13 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaApplianceServiceRolePolicy

Descripción: Permite que un dispositivo AWS Panorama cargue registros en Amazon CloudWatch y obtenga objetos de los puntos de acceso de Amazon S3 creados para su uso con AWS Panorama.

`AWSPanoramaApplianceServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaApplianceServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 20 de octubre de 2021 a las 12:14 UTC
- Hora de edición: 10 de diciembre de 2024 a las 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaFullAccess

Descripción: Proporciona acceso completo a AWS Panorama

`AWSPanoramaFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2020 a las 13:12 UTC
- Hora editada: 10 de diciembre de 2024 a las 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaGreengrassGroupRolePolicy

Descripción: Permite que una función AWS Lambda de un dispositivo AWS Panorama gestione los recursos de Panorama, suba registros y métricas a Amazon CloudWatch y gestione los objetos de los depósitos creados para su uso con Panorama.

`AWSPanoramaGreengrassGroupRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaGreengrassGroupRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:10 UTC
- Hora de edición: 6 de enero de 2021 a las 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaSageMakerRolePolicy

Descripción: Permite SageMaker a Amazon gestionar objetos en depósitos creados para su uso con AWS Panorama.

`AWSPanoramaSageMakerRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaSageMakerRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 1 de diciembre de 2020 a las 13:13 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaServiceLinkedRolePolicy

Descripción: Permite a AWS Panorama gestionar los recursos en AWS IoT, AWS Secrets Manager y AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de octubre de 2021 a las 12:12 UTC
- Hora de edición: 20 de octubre de 2021 a las 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPanoramaServiceRolePolicy

Descripción: Permite a AWS Panorama gestionar los recursos en Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda SageMaker, Amazon y Amazon CloudWatch Logs, y transferir las funciones de servicio a AWS IoT GreenGrass, AWS IoT y Amazon. SageMaker

`AWSPanoramaServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPanoramaServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de diciembre de 2020 a las 13:14 UTC
- Hora de edición: 1 de diciembre de 2020 a las 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPartnerCentralFullAccess

Descripción: Proporciona acceso completo a AWS Partner Central y otros sitios relacionados Servicios de AWS.

`AWSPartnerCentralFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPartnerCentralFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de noviembre de 2024 a las 23:33 UTC
- Hora editada: 10 de diciembre de 2024 a las 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPartnerCentralOpportunityManagement

Descripción: Proporciona el acceso necesario para las actividades de gestión de oportunidades.

`AWSPartnerCentralOpportunityManagement` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPartnerCentralOpportunityManagement` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de noviembre de 2024 a las 19:09 UTC
- Hora editada: 4 de diciembre de 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
```

```
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPartnerCentralSandboxFullAccess

Descripción: Proporciona el acceso necesario para que los desarrolladores realicen pruebas en el catálogo de Sandbox.

`AWSPartnerCentralSandboxFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPartnerCentralSandboxFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de noviembre de 2024 a las 19:10 UTC
- Hora editada: 10 de diciembre de 2024 a las 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Descripción: Proporciona acceso al recurso ResourceSnapshotJob para leer y hacer una instantánea de él en la interacción objetivo.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de diciembre de 2024 a las 18:21 UTC
- Hora editada: 10 de diciembre de 2024 a las 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPartnerLedSupportReadOnlyAccess

Descripción: Esta política se puede utilizar para conceder un acceso de solo lectura APIs que pueda leer los metadatos de los servicios de su empresa. Cuenta de AWS Puede utilizar esta política para proporcionar a sus socios del Partner-Led Support Program acceso a los servicios que se especifican en la sección de detalles de permisos que aparece a continuación.

`AWSPartnerLedSupportReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPartnerLedSupportReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de noviembre de 2024 a las 20:06 UTC
- Hora editada: 22 de noviembre de 2024 a las 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPCSComputeNodePolicy

Descripción: Concede permiso a los nodos de cómputo de AWS PCS para conectarse a los clústeres de AWS PCS.

`AWSPCSComputeNodePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPCSComputeNodePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 23 de junio de 2025 a las 18:07 UTC
- Hora editada: 23 de junio de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPCSServiceRolePolicy

Descripción: concede permisos a PCS para administrar recursos en su nombre.

`AWSPCSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de agosto de 2024 a las 16:01 h UTC
- Hora de edición: 27 de agosto de 2024 a las 16:01 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPriceListServiceFullAccess

Descripción: Proporciona acceso completo al servicio de lista de AWS precios.

`AWSPriceListServiceFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPriceListServiceFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de noviembre de 2017 a las 00:36 UTC
- Hora de edición: 02 de julio de 2024 a las 13:34 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAAuditor

Descripción: Proporciona acceso de auditor a una autoridad de certificación AWS privada

`AWSPrivateCAAuditor` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAAuditor` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de febrero de 2023 a las 18:33 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAConnectorForKubernetesPolicy

Descripción: Otorga los permisos esenciales para el conector de CA AWS privado para Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAConnectorForKubernetesPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de mayo de 2025 a las 19:22 UTC
- Hora editada: 19 de mayo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAFullAccess

Descripción: Proporciona acceso completo a la autoridad de certificación AWS privada

`AWSPrivateCAFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de febrero de 2023 a las 18:20 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAPrivilegedUser

Descripción: Proporciona a los usuarios de certificados privilegiados acceso a una autoridad de certificación AWS privada

`AWSPrivateCAPrivilegedUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAPrivilegedUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de febrero de 2023 a las 18:26 UTC
- Hora editada: 22 de enero de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAReadOnly

Descripción: Proporciona acceso de solo lectura a la autoridad de certificación AWS privada

`AWSPrivateCAReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de febrero de 2023 a las 18:30 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:30 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateCAUser

Descripción: Proporciona a los usuarios de certificados acceso a una autoridad de certificación AWS privada

`AWSPrivateCAUser` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateCAUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de febrero de 2023 a las 18:16 UTC
- Hora editada: 22 de enero de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateMarketplaceAdminFullAccess

Descripción: Proporciona acceso completo a todas las acciones administrativas de un Marketplace AWS privado.

`AWSPrivateMarketplaceAdminFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateMarketplaceAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 16:32 UTC
- Hora editada: 11 de junio de 2025 a las 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateMarketplaceRequests

Descripción: Proporciona acceso a la creación de solicitudes en un Marketplace AWS privado.

`AWSPrivateMarketplaceRequests` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPrivateMarketplaceRequests` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de octubre de 2019 a las 21:44 UTC
- Hora de edición: 28 de octubre de 2019 a las 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPrivateNetworksServiceRolePolicy

Descripción: Permite que AWS Private Networks Service administre los recursos en nombre del cliente.

`AWSPrivateNetworksServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de diciembre de 2021 a las 23:17 UTC
- Hora de edición: 16 de diciembre de 2021 a las 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonCodeBuildProvisioningBasicAccess

Descripción: Se CodeBuild necesitan permisos para ejecutar una compilación de AWS Proton Provisioning CodeBuild .

`AWSProtonCodeBuildProvisioningBasicAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSProtonCodeBuildProvisioningBasicAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 9 de noviembre de 2022 a las 21:04 UTC
- Hora de edición: 09 de noviembre de 2022 a las 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonCodeBuildProvisioningServiceRolePolicy

Descripción: Permite a AWS Proton administrar el aprovisionamiento de recursos de Proton utilizando CodeBuild y otros AWS servicios en su nombre.

`AWSProtonCodeBuildProvisioningServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2022 a las 21:32 UTC
- Hora de edición: 17 de mayo de 2023 a las 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonDeveloperAccess

Descripción: Proporciona acceso a AWS Proton APIs y a la consola de administración, pero no permite la administración de plantillas o entornos de Proton.

`AWSProtonDeveloperAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSProtonDeveloperAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 17 de febrero de 2021 a las 19:02 UTC
- Hora de edición: 06 de junio de 2024 a las 18:26 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonFullAccess

Descripción: Proporciona acceso completo a AWS Proton APIs y a la consola de administración. Además de estos permisos, también es necesario acceder a Amazon S3 para registrar las agrupaciones de plantillas de sus buckets de S3. Asimismo, se precisa acceder a Amazon IAM para crear y administrar los roles de servicio de Proton.

`AWSProtonFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSProtonFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de febrero de 2021 a las 19:07 UTC
- Hora de edición: 06 de junio de 2024 a las 18:29 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Proton APIs y a la consola de administración.

`AWSProtonReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSProtonReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de febrero de 2021 a las 19:09 UTC
- Hora de edición: 18 de noviembre de 2022 a las 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonServiceGitSyncServiceRolePolicy

Descripción: Política que permite a AWS Proton sincronizar sus definiciones de servicio, entorno y componentes de su repositorio de git con AWS Proton.

`AWSProtonServiceGitSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de abril de 2023 a las 15:55 UTC
- Hora de edición: 04 de abril de 2023 a las 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSProtonSyncServiceRolePolicy

Descripción: Política que permite a AWS Proton sincronizar el contenido de su repositorio de git con Proton o sincronizar el contenido de Proton con sus repositorios de git.

`AWSProtonSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de noviembre de 2021 a las 21:14 UTC
- Hora de edición: 05 de mayo de 2024 a las 01:49 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSPurchaseOrdersServiceRolePolicy

Descripción: concede permisos para ver y modificar los pedidos de compra en la consola de facturación

`AWSPurchaseOrdersServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSPurchaseOrdersServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de mayo de 2020 a las 18:15 UTC
- Hora editada: 1 de diciembre de 2024 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupCFGCPacksPermissionsBoundary

Descripción: La CFGCPacks PermissionsBoundary política de AWSQuick configuración define la lista de permisos permitidos en un rol de IAM creado por Quick Setup. La configuración rápida utiliza un rol creado con esta política para implementar los paquetes de conformidad de AWS Config.

`AWSQuickSetupCFGCPacksPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupCFGCPacksPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:52 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:52 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupDeploymentRolePolicy

Descripción: Proporciona permisos para que AWS Systems Manager Quick Setup implemente varios tipos de configuración. Estos tipos de configuración crean roles y automatizaciones de IAM que configuran servicios y características de Amazon Web Services utilizados con frecuencia, mediante las prácticas recomendadas.

`AWSQuickSetupDeploymentRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupDeploymentRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:55 h UTC
- Hora editada: 10 de junio de 2025 a las 13:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    },
    {
      "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: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"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupDevOpsGuruPermissionsBoundary

Descripción: La AWSQuick SetupDevOpsGuruPermissionsBoundary política define la lista de permisos permitidos en un rol de IAM creado por Quick Setup. Quick Setup usa un rol creado con

esta política para habilitar y configurar Amazon DevOps Guru. Esta política también proporciona permisos para habilitar Systems Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupDevOpsGuruPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:44 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:44 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupDistributorPermissionsBoundary

Descripción: QuickSetup crea funciones de IAM que le permiten configurar la función de distribuidor de Systems Manager en su nombre y utiliza esta política al crear dichas funciones para definir el límite de sus permisos.

`AWSQuickSetupDistributorPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupDistributorPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:50 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:50 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupEnableAREXExecutionPolicy

Descripción: Esta política concede permisos que permiten a Systems Manager ejecutar el manual de AWSQuickSetupType-EnableAREX automatización, lo que permite utilizar AWS Resource Explorer con Systems Manager.

`AWSQuickSetupEnableAREXExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupEnableAREXExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de noviembre de 2024 a las 22:45 UTC
- Hora editada: 15 de noviembre de 2024 a las 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupEnableDHMCExecutionPolicy

Descripción: Esta política otorga permisos que permiten a los directores ejecutar el manual de AWSQuickSetupType-EnableDHMC automatización, que habilita la configuración de administración de hosts predeterminada.

`AWSQuickSetupEnableDHMCExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupEnableDHMCExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 21:27 UTC
- Hora editada: 15 de noviembre de 2024 a las 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupJITNADeploymentRolePolicy

Descripción: Esta política permite a Quick Setup implementar el tipo de configuración necesario para configurar el acceso a los just-in-time nodos.

`AWSQuickSetupJITNADeploymentRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupJITNADeploymentRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de abril de 2025 a las 09:07 UTC
- Hora editada: 17 de abril de 2025, 09:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Descripción: Esta política concede permisos administrativos que permiten a Systems Manager crear un perfil de instancia de IAM predeterminado para la capacidad de configuración rápida y adjuntarlo a las EC2 instancias de Amazon que aún no tienen un perfil de instancia adjunto.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupManagedInstanceProfileExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 21:51 UTC
- Hora editada: 15 de noviembre de 2024 a las 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.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"
          ]
```

```
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "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"
          ]
        }
      }
    },
    {
      "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"
          ]
        }
      }
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Descripción: Esta política proporciona permisos para habilitar el acceso a los just-in-time nodos para Systems Manager.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupManageJITNAResourcesExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de abril de 2025 a las 21:37 UTC
- Hora editada: 23 de abril de 2025 a las 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

```
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupPatchPolicyBaselineAccess

Descripción: Proporciona permisos de solo lectura para acceder a las líneas base de parches configuradas por un administrador de la organización Cuenta de AWS o entidad actual mediante la configuración rápida.

`AWSQuickSetupPatchPolicyBaselineAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupPatchPolicyBaselineAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 26 de junio de 2024 a las 09:38 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:38 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Descripción: proporciona permisos que permiten que la Configuración rápida cree recursos asociados a la configuración de la política de revisiones.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupPatchPolicyDeploymentRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:57 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:57 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupPatchPolicyPermissionsBoundary

Descripción: QuickSetup crea funciones de IAM que le permiten configurar la función Systems Manager Patch Manager en su nombre y utiliza esta política al crear dichas funciones para definir el límite de sus permisos.

`AWSQuickSetupPatchPolicyPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupPatchPolicyPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:46 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:46 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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-*"
      ]
    },
    {
```

```
      "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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSchedulerPermissionsBoundary

Descripción: La AWSQuick SetupSchedulerPermissionsBoundary política define la lista de permisos permitidos en un rol de IAM creado por Quick Setup. Quick Setup usa un rol creado con esta política para habilitar y configurar las operaciones programadas en las EC2 instancias de Amazon y otros recursos.

`AWSQuickSetupSchedulerPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSchedulerPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:53 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:53 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSSMDeploymentRolePolicy

Descripción: Esta política otorga permisos administrativos que permiten a Quick Setup crear recursos que se utilizan durante el proceso de incorporación de Systems Manager.

`AWSQuickSetupSSMDeploymentRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSSMDeploymentRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 22:53 UTC
- Hora editada: 5 de mayo de 2025 a las 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Descripción: Esta política otorga permisos para incluir todos los depósitos de S3 de una cuenta y para administrar y recuperar información sobre grupos específicos de la cuenta principal que se administran mediante plantillas. AWS CloudFormation

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 22:01 UTC
- Hora editada: 15 de noviembre de 2024 a las 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Descripción: la Configuración rápida crea roles de IAM que le permiten configurar el tipo de Configuración rápida del Administrador de hosts en su nombre. Además, utiliza esta política al crear dichos roles para definir el límite de sus permisos.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSSMHostMgmtPermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:48 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:48 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Descripción: La política concede permisos administrativos que permiten a Quick Setup ejecutar un recurso AWS CloudFormation personalizado en eventos del ciclo de vida durante la implementación de Quick Setup en Systems Manager.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de noviembre de 2024 a las 21:55 UTC
- Hora editada: 15 de noviembre de 2024 a las 21:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSetupSSMManageResourcesExecutionPolicy

Descripción: Esta política otorga permisos que permiten a Systems Manager crear requisitos previos, como las funciones de IAM necesarias para la incorporación de Systems Manager.

`AWSQuickSetupSSMManageResourcesExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSetupSSMManageResourcesExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 15 de noviembre de 2024 a las 22:49 UTC
- Hora editada: 15 de noviembre de 2024 a las 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightAssetBundleExportPolicy

Descripción: Proporciona el conjunto de permisos necesarios para realizar operaciones de exportación de paquetes de QuickSight activos

`AWSQuickSightAssetBundleExportPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightAssetBundleExportPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de marzo de 2024 a las 21:31 h UTC
- Hora de edición: 27 de marzo de 2024 a las 21:31 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightAssetBundleImportPolicy

Descripción: Proporciona el conjunto de permisos necesarios para realizar operaciones de importación de paquetes de QuickSight activos

`AWSQuickSightAssetBundleImportPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightAssetBundleImportPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de marzo de 2024 a las 21:40 h UTC
- Hora de edición: 27 de marzo de 2024 a las 21:40 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuicksightAthenaAccess

Descripción: acceso de Quicksight a la API de Athena y a los buckets de S3 utilizados para los resultados de las consultas de Athena

`AWSQuicksightAthenaAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuicksightAthenaAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de diciembre de 2016 a las 02:31 UTC
- Hora editada: 3 de enero de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightDescribeRDS

Descripción: Permite QuickSight describir los recursos de RDS

`AWSQuickSightDescribeRDS` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightDescribeRDS` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:24 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightDescribeRedshift

Descripción: Permite describir QuickSight los recursos de Redshift

`AWSQuickSightDescribeRedshift` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightDescribeRedshift` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:25 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightElasticsearchPolicy

Descripción: Proporciona acceso a los recursos de Amazon Elasticsearch desde Amazon QuickSight

`AWSQuickSightElasticsearchPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightElasticsearchPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 9 de septiembre de 2020 a las 17:27 UTC

- Hora de edición: 7 de septiembre de 2021 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightIoTAnalyticsAccess

Descripción: Otorgar acceso de QuickSight solo lectura a los conjuntos de datos de IoT Analytics

`AWSQuickSightIoTAnalyticsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightIoTAnalyticsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2017 a las 17:00 UTC

- Hora de edición: 29 de noviembre de 2017 a las 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightListIAM

Descripción: Permite QuickSight enumerar las entidades de IAM

`AWSQuickSightListIAM` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightListIAM` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 10 de noviembre de 2015 a las 23:25 UTC
- Hora de edición: 10 de noviembre de 2015 a las 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuicksightOpenSearchPolicy

Descripción: Proporciona acceso a los OpenSearch recursos de Amazon desde Amazon QuickSight

`AWSQuicksightOpenSearchPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuicksightOpenSearchPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 7 de septiembre de 2021 a las 23:26 UTC
- Hora de edición: 7 de septiembre de 2021 a las 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightSageMakerPolicy

Descripción: Proporciona acceso a los SageMaker recursos de Amazon desde Amazon QuickSight

`AWSQuickSightSageMakerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightSageMakerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 17 de enero de 2020 a las 17:18 UTC
- Hora de edición: 30 de octubre de 2023 a las 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightSecretsManagerWriteAccess

Descripción: Política utilizada por QuickSight para crear AWS secretos en Secrets Manager y adjuntar políticas de recursos a QuickSight los secretos existentes.

`AWSQuickSightSecretsManagerWriteAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightSecretsManagerWriteAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 22 de mayo de 2025 a las 01:22 UTC
- Hora editada: 22 de mayo de 2025 a las 01:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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!*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightSecretsManagerWritePolicy

Descripción: Política utilizada por QuickSight para crear AWS secretos en Secrets Manager y adjuntar políticas de recursos a QuickSight los secretos existentes.

`AWSQuickSightSecretsManagerWritePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightSecretsManagerWritePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de mayo de 2025 a las 19:22 UTC
- Hora editada: 12 de mayo de 2025 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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!*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSQuickSightTimestreamPolicy

Descripción: AWS QuickSight acceso a AWS Timestream APIs. Los clientes pueden adjuntar esta política a su AWS QuickSight rol para permitir la recuperación de datos y metadatos.

`AWSQuickSightTimestreamPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSQuickSightTimestreamPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 30 de septiembre de 2020 a las 21:47 UTC
- Hora de edición: 30 de septiembre de 2020 a las 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSReachabilityAnalyzerServiceRolePolicy

Descripción: Permite que VPC Reachability Analyzer AWS acceda a los recursos y se integre con Organizations en su nombre. AWS

`AWSReachabilityAnalyzerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 23 de noviembre de 2022 a las 17:12 UTC
- Hora de edición: 10 de septiembre de 2024 a las 16:04 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRefactoringToolkitFullAccess

Descripción: esta política otorga permiso para usar los AWS servicios con la extensión AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. Está pensado para adjuntarse a un perfil local. AWS La política permite cargar artefactos de aplicaciones y descargar los artefactos resultantes de Amazon S3. Permite crear aplicaciones en una imagen de contenedor utilizando, almacenar AWS CodeBuild y recuperar las imágenes de Amazon Elastic Container Registry (Amazon ECR). Además, permite el despliegue de la aplicación en servicios de contenedores, AWS como Amazon Elastic Container Service (Amazon ECS), la creación opcional de recursos de VPC, la conexión opcional a la infraestructura existente, como Directory AWS Service, y otros servicios relacionados.

`AWSRefactoringToolkitFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRefactoringToolkitFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de octubre de 2022 a las 16:41 UTC
- Hora editada: 9 de abril de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRefactoringToolkitSidecarPolicy

Descripción: Esta política está destinada a las tareas de Amazon ECS creadas para probar aplicaciones AWS con la extensión AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. La política otorga acceso para descargar artefactos de aplicaciones desde Amazon S3, comunicar el estado de la tarea mediante AWS Systems Manager y otros servicios necesarios.

`AWSRefactoringToolkitSidecarPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRefactoringToolkitSidecarPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de octubre de 2022 a las 16:41 UTC
- Hora de edición: 29 de octubre de 2022 a las 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSrePostPrivateCloudWatchAccess

Descripción: Proporciona acceso privado a Re:post para publicar datos de métricas CloudWatch

`AWSrePostPrivateCloudWatchAccess` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2023 a las 16:37 UTC
- Hora de edición: 15 de noviembre de 2023 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRepostSpaceSupportOperationsPolicy

Descripción: esta política permite al servicio re:Post Space crear, administrar y resolver los casos de soporte que se crean a través de la aplicación Space.

`AWSRepostSpaceSupportOperationsPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRepostSpaceSupportOperationsPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de noviembre de 2023 a las 21:52 h UTC
- Hora de edición: 26 de noviembre de 2023 a las 21:52 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResilienceHubAsssessmentExecutionPolicy

Descripción: Política para AWS la función de servicio de Resilience Hub que permite el acceso a otros AWS servicios para ejecutar la evaluación.

`AWSResilienceHubAsssessmentExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResilienceHubAsssessmentExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2023 a las 12:32 UTC
- Hora editada: 16 de diciembre de 2024 a las 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceAccessManagerFullAccess

Descripción: Proporciona acceso completo a AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceAccessManagerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de junio de 2019 a las 17:28 UTC
- Hora de edición: 4 de junio de 2019 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceAccessManagerReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceAccessManagerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de diciembre de 2019 a las 20:58 UTC
- Hora de edición: 9 de diciembre de 2019 a las 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceAccessManagerResourceShareParticipantAccess

Descripción: Proporciona acceso al AWS Resource Access Manager APIs que necesita un participante de un recurso compartido.

`AWSResourceAccessManagerResourceShareParticipantAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceAccessManagerResourceShareParticipantAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de diciembre de 2019 a las 20:41 UTC

- Hora de edición: 9 de diciembre de 2019 a las 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceAccessManagerServiceRolePolicy

Descripción: Política que contiene el acceso de AWS Resource Access Manager de solo lectura a la estructura de Organizations de los clientes. También, contiene permisos de IAM para eliminar el rol.

`AWSResourceAccessManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 19:28 UTC
- Hora de edición: 14 de noviembre de 2018 a las 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceExplorerFullAccess

Descripción: Esta política concede permisos administrativos para acceder a los recursos del Explorador de recursos y concede permisos de solo lectura a otros AWS servicios para permitir este acceso.

`AWSResourceExplorerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceExplorerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 7 de noviembre de 2022 a las 20:01 UTC
- Hora de edición: 14 de noviembre de 2023 a las 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceExplorerOrganizationsAccess

Descripción: Esta política concede permisos administrativos al Explorador de recursos y concede permisos de solo lectura a otros AWS servicios para admitir este acceso. El administrador de AWS Organizations necesita estos permisos para configurar y administrar la búsqueda de varias cuentas en la consola.

`AWSResourceExplorerOrganizationsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceExplorerOrganizationsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 14 de noviembre de 2023 a las 17:01 UTC
- Hora de edición: 14 de noviembre de 2023 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceExplorerReadOnlyAccess

Descripción: Esta política concede permisos de solo lectura para buscar y ver los recursos del Explorador de recursos y concede permisos de solo lectura a otros AWS servicios para respaldar este acceso.

`AWSResourceExplorerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceExplorerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 7 de noviembre de 2022 a las 19:56 UTC
- Hora de edición: 14 de noviembre de 2023 a las 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceExplorerServiceRolePolicy

Descripción: Permite que Resource Explorer vea los recursos y CloudTrail eventos en su nombre para indexarlos para su búsqueda.

`AWSResourceExplorerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de octubre de 2022 a las 20:35 UTC
- Hora editada: 23 de junio de 2025 a las 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appflow:ListFlows",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
```

```
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessments",
        "autoscaling:DescribeAutoScalingGroups",
        "backup-gateway:ListHypervisors",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "bedrock:ListAgents",
        "bedrock:ListBlueprints",
        "bedrock:ListCustomModels",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListVoiceConnectors",
        "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",
        "cloudtrail:ListChannels",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:ListConnections",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:ListPipelines",
        "codepipeline:ListWebhooks",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "config:DescribeConfigRules",
        "connect:ListHoursOfOperations",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
```

```
        "datasync:ListLocations",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "detective:ListGraphs",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeLags",
        "directconnect:DescribeVirtualInterfaces",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "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: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:DescribeVpcEndpointServices",
        "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",
        "ecs:ListTasks",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "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",
        "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:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "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:ListMLTransforms",
        "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:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "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:ListScenes",
        "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:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
```

```
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "managedblockchain:ListAccessors",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "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",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
```

```
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots",
        "outposts:ListSites",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "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:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListSafetyRules",
        "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",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
```

```
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "timestream:ListDatabases",
        "timestream:ListScheduledQueries",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
```

```
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "wafv2:ListWebACLs",
        "wisdom:ListAssistants",
        "wisdom:listAssistantAssociations",
        "wisdom:listKnowledgeBases",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSResourceGroupsReadOnlyAccess

Descripción: Esta es la política de solo lectura para AWS Resource Groups

`AWSResourceGroupsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSResourceGroupsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de marzo de 2018 a las 10:27 UTC
- Hora de edición: 5 de febrero de 2019 a las 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRoboMaker_FullAccess

Descripción: Proporciona acceso completo a AWS RoboMaker través del SDK AWS Management Console y. También, brinda acceso selecto a servicios relacionados (por ejemplo, S3 o IAM).

`AWSRoboMaker_FullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRoboMaker_FullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de septiembre de 2020 a las 18:34 UTC
- Hora de edición: 16 de septiembre de 2021 a las 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRoboMakerReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS RoboMaker través del AWS Management Console SDK

`AWSRoboMakerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRoboMakerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de noviembre de 2018 a las 05:30 UTC
- Hora de edición: 28 de agosto de 2020 a las 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRoboMakerServicePolicy

Descripción: política RoboMaker de servicio

`AWSRoboMakerServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 06:30 UTC
- Hora de edición: 11 de noviembre de 2021 a las 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRoboMakerServiceRolePolicy

Descripción: política RoboMaker de servicio

`AWSRoboMakerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSRoboMakerServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de noviembre de 2018 a las 05:33 UTC
- Hora de edición: 26 de noviembre de 2018 a las 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSRolesAnywhereServicePolicy

Descripción: Permite a IAM Roles Anywhere publicar métricas de servicio y uso CloudWatch y comprobar el estado de las autoridades de certificación privadas en su nombre.

`AWSRolesAnywhereServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de julio de 2022 a las 15:26 UTC
- Hora de edición: 5 de julio de 2022 a las 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSS3OnOutpostsServiceRolePolicy

Descripción: Permita que Amazon S3 on Outposts administre los recursos de la EC2 red en su nombre.

`AWSS3OnOutpostsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 3 de octubre de 2023 a las 20:32 UTC
- Hora de edición: 3 de octubre de 2023 a las 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSavingsPlansFullAccess

Descripción: proporciona acceso completo al servicio de Savings Plans

`AWSSavingsPlansFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSavingsPlansFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de noviembre de 2019 a las 22:45 UTC
- Hora de edición: 6 de noviembre de 2019 a las 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSavingsPlansReadOnlyAccess

Descripción: proporciona acceso de solo lectura al servicio de Savings Plans

`AWSSavingsPlansReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSavingsPlansReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de noviembre de 2019 a las 22:45 UTC
- Hora de edición: 6 de noviembre de 2019 a las 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityHubFullAccess

Descripción: Proporciona acceso completo para usar AWS Security Hub.

`AWSSecurityHubFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityHubFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 27 de noviembre de 2018 a las 23:54 UTC
- Hora editada: 17 de junio de 2025 a las 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityHubOrganizationsAccess

Descripción: Otorga permiso para habilitar y administrar AWS Security Hub dentro de una organización. Incluye habilitar el servicio en toda la organización y determinar una cuenta como administrador delegado para el servicio.

`AWSSecurityHubOrganizationsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityHubOrganizationsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de marzo de 2021 a las 20:53 UTC
- Hora editada: 24 de junio de 2025 a las 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.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/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : "SECURITYHUB_POLICY"
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityHubReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los recursos AWS de Security Hub

`AWSSecurityHubReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityHubReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2018 a las 01:34 UTC
- Hora de edición: 22 de febrero de 2024 a las 23:45 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityHubServiceRolePolicy

Descripción: Se requiere un rol vinculado a un servicio para que AWS Security Hub acceda a sus recursos.

`AWSSecurityHubServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2018 a las 23:47 UTC
- Hora de edición: 27 de noviembre de 2023 a las 03:46 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityHubV2ServiceRolePolicy

Descripción: Esta política permite a Security Hub gestionar las reglas de AWS configuración y los recursos del Security Hub en su organización y en su nombre.

`AWSSecurityHubV2ServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de junio de 2025 a las 17:37 UTC
- Hora editada: 10 de junio de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*"
    },
    {
      "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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityIncidentResponseCaseFullAccess

Descripción: La política proporciona a los clientes permisos de lectura y escritura sobre los recursos de casos que se crean mediante el servicio de respuesta a incidentes de seguridad.

`AWSSecurityIncidentResponseCaseFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityIncidentResponseCaseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2024 a las 23:21 UTC
- Hora editada: 1 de diciembre de 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIRCaseWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityIRCaseTagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityIncidentResponseFullAccess

Descripción: La política proporciona a los clientes permisos de lectura y escritura para acceder a todos los recursos asociados al servicio de respuesta a incidentes de seguridad.

`AWSSecurityIncidentResponseFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityIncidentResponseFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2024 a las 23:21 UTC
- Hora editada: 1 de diciembre de 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "security-ir:CancelMembership",
        "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:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
```

```
        }
      }
    },
    {
      "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"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityIncidentResponseReadOnlyAccess

Descripción: La política proporciona a los clientes permisos de solo lectura para todos los recursos asociados al servicio de respuesta a incidentes de seguridad. El permiso también incluye el acceso GetCaseAttachmentDownloadUrl a la descarga de los archivos adjuntos de la funda. URLs

`AWSSecurityIncidentResponseReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSecurityIncidentResponseReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2024 a las 23:06 UTC
- Hora editada: 1 de diciembre de 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityIncidentResponseServiceRolePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por Security Incident Response

`AWSSecurityIncidentResponseServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2024 a las 16:36 UTC
- Hora editada: 1 de diciembre de 2024, 16:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
```

```
        "organizations:ListChildren"
      ],
      "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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSecurityIncidentResponseTriageServiceRolePolicy

Descripción: Proporciona acceso a la respuesta a incidentes de AWS seguridad para monitorear continuamente su entorno en busca de amenazas a la seguridad, ajustar los servicios de seguridad para reducir el ruido de las alertas y recopilar información para investigar posibles incidentes.

`AWSSecurityIncidentResponseTriageServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2024 a las 16:36 UTC
- Hora editada: 2 de junio de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogAdminFullAccess

Descripción: proporciona acceso completo a las capacidades de administración de Service Catalog

`AWSServiceCatalogAdminFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogAdminFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de febrero de 2018 a las 17:19 UTC
- Hora de edición: 13 de abril de 2023 a las 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogAdminReadOnlyAccess

Descripción: proporciona acceso de solo lectura a las capacidades de administración de Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogAdminReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de octubre de 2019 a las 18:53 UTC
- Hora de edición: 25 de octubre de 2019 a las 18:53 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogAppRegistryFullAccess

Descripción: proporciona acceso completo a las capacidades de Registro de aplicaciones de Service Catalog

`AWSServiceCatalogAppRegistryFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogAppRegistryFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de noviembre de 2020 a las 22:25 UTC
- Hora de edición: 7 de diciembre de 2023 a las 21:50 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*:*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogAppRegistryReadOnlyAccess

Descripción: proporciona acceso de solo lectura a las capacidades de Registro de aplicaciones de Service Catalog

`AWSServiceCatalogAppRegistryReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogAppRegistryReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de noviembre de 2020 a las 22:34 UTC
- Hora de edición: 17 de noviembre de 2022 a las 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogAppRegistryServiceRolePolicy

Descripción: Permite que Service Catalog AppRegistry administre los grupos de recursos en su nombre

`AWSServiceCatalogAppRegistryServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de mayo de 2021 a las 22:18 UTC
- Hora de edición: 26 de octubre de 2022 a las 16:05 UTC

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

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogEndUserFullAccess

Descripción: proporciona acceso completo a las capacidades de usuario final de Service Catalog

`AWSServiceCatalogEndUserFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogEndUserFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 15 de febrero de 2018 a las 17:22 UTC
- Hora de edición: 10 de julio de 2019 a las 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogEndUserReadOnlyAccess

Descripción: proporciona acceso de solo lectura a las capacidades de usuario final de Service Catalog

`AWSServiceCatalogEndUserReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSServiceCatalogEndUserReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 25 de octubre de 2019 a las 18:49 UTC
- Hora de edición: 25 de octubre de 2019 a las 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Descripción: Una política de roles vinculados a servicios para AWS ServiceCatalog sincronizarla con la estructura AWS organizativa de las organizaciones

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de abril de 2023 a las 20:48 UTC
- Hora de edición: 10 de abril de 2023 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceCatalogSyncServiceRolePolicy

Descripción: Una función vinculada a un servicio AWS ServiceCatalog para sincronizar los artefactos de aprovisionamiento de los repositorios de origen

`AWSServiceCatalogSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2022 a las 21:20 UTC

- Hora de edición: 03 de mayo de 2024 a las 17:12 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForAmazonEKSNodegroup

Descripción: se requieren permisos para administrar grupos de nodos en la cuenta del cliente. Estas políticas están relacionadas con la administración de los siguientes recursos: AutoscalingGroups SecurityGroups, LaunchTemplates y InstanceProfiles.

`AWSServiceRoleForAmazonEKSNodegroup` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de noviembre de 2019 a las 01:34 UTC
- Hora editada: 21 de noviembre de 2024 a las 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
      ],
      "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/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForAmazonQDeveloper

Descripción: este rol vinculado al servicio proporciona a Amazon Q Developer la posibilidad de proporcionar información de uso.

`AWSServiceRoleForAmazonQDeveloper` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de abril de 2024 a las 07:40 h UTC
- Hora de edición: 25 de abril de 2024 a las 07:40 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForAWSTransform

Descripción: Esta función vinculada al servicio proporciona a AWS Transform la capacidad de proporcionar información de uso.

`AWSServiceRoleForAWSTransform` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de mayo de 2025 a las 13:37 UTC
- Hora editada: 15 de mayo de 2025 a las 13:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Descripción: Proporciona acceso a los recursos de Systems Manager utilizados por CloudWatch Alarms

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de octubre de 2020 a las 09:49 UTC
- Hora de edición: 1 de octubre de 2020 a las 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Descripción: Permite acceder CloudWatch a las métricas de RDS Performance Insights en su nombre

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2023 a las 09:32 UTC
- Hora de edición: 07 de septiembre de 2023 a las 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForCodeGuru-Profiler

Descripción: Amazon CodeGuru Profiler necesita un rol vinculado a un servicio para enviar notificaciones en su nombre.

`AWSServiceRoleForCodeGuru-Profiler` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de junio de 2020 a las 22:04 UTC
- Hora de edición: 26 de junio de 2020 a las 22:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForCodeWhispererPolicy

Descripción: Esta función otorga permisos para acceder CodeWhisperer a los datos de tu cuenta para calcular la facturación, proporciona acceso para crear y acceder a informes de seguridad en Amazon CodeGuru y emite datos a CloudWatch.

`AWSServiceRoleForCodeWhispererPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de marzo de 2023 a las 19:39 UTC
- Hora de edición: 29 de marzo de 2024 a las 22:13 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForEC2ScheduledInstances

Descripción: Permite a EC2 Scheduled Instances lanzar y gestionar instancias puntuales.

`AWSServiceRoleForEC2ScheduledInstances` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de octubre de 2017 a las 18:31 UTC
- Hora de edición: 12 de octubre de 2017 a las 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Descripción: AWS GroundStation utiliza este rol vinculado al servicio para EC2 invocar y buscar direcciones públicas IPv4

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de diciembre de 2022 a las 23:52 UTC
- Hora de edición: 13 de diciembre de 2022 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForImageBuilder

Descripción: Permite llamar EC2 ImageBuilder a AWS los servicios en su nombre.

`AWSServiceRoleForImageBuilder` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2019 a las 22:02 UTC
- Hora editada: 26 de diciembre de 2024 a las 23:52 UTC

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

Versión de la política

Versión de la política: v20 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "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" : [
        "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-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForIoTSiteWise

Descripción: Permite SiteWise al AWS IoT aprovisionar y gestionar pasarelas, así como consultar datos. La política incluye los permisos de AWS Greengrass necesarios para realizar despliegues en grupos, los permisos de AWS Lambda para crear y actualizar funciones con prefijo de servicio y los permisos de IoT AWS Analytics para consultar datos de almacenes de datos.

`AWSServiceRoleForIoTSiteWise` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2018 a las 19:19 UTC

- Hora de edición: 13 de noviembre de 2023 a las 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForLogDeliveryPolicy

Descripción: permite que el Servicio de entrega de registros los entregue al llamar al destino del registro en su nombre.

`AWSServiceRoleForLogDeliveryPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de octubre de 2019 a las 17:31 UTC
- Hora editada: 16 de enero de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForMonitronPolicy

Descripción: Otorga a Amazon Monitron permisos para administrar los AWS recursos, incluida la asignación de usuarios de AWS SSO en su nombre.

`AWSServiceRoleForMonitronPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de diciembre de 2020 a las 19:06 UTC
- Hora de edición: 02 de octubre de 2024 a las 10:06 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForNeptuneGraphPolicy

Descripción: proporciona a Cloudwatch acceso para publicar registros y métricas operativas y de uso para Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2023 a las 14:03 h UTC
- Hora de edición: 29 de noviembre de 2023 a las 14:03 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Descripción: Proporciona permisos para describir y actualizar los recursos de Private Marketplace y describir AWS las organizaciones

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de febrero de 2024 a las 22:28 h UTC
- Hora de edición: 14 de febrero de 2024 a las 22:28 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForProcurementInsightsPolicy

Descripción: política para que Información de compras obtenga detalles de la cuenta de la organización

`AWSServiceRoleForProcurementInsightsPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 03 de octubre de 2024 a las 14:26 h UTC
- Hora de edición: 03 de octubre de 2024 a las 14:26 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForSMS

Descripción: Proporciona acceso a AWS los servicios y recursos necesarios para migrar las instancias de servicio a S3 y Cloudformation EC2, AWS incluidas.

`AWSServiceRoleForSMS` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de agosto de 2019 a las 18:39 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRoleForUserSubscriptions

Descripción: proporciona acceso al servicio de suscripciones de usuarios a los recursos de Identity Center para actualizar automáticamente las suscripciones.

`AWSServiceRoleForUserSubscriptions` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de abril de 2024 a las 16:14 h UTC
- Hora editada: 21 de febrero de 2025 a las 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRolePolicyForBackupReports

Descripción: Proporciona permisos AWS de Backup para crear informes de conformidad en su nombre

`AWSServiceRolePolicyForBackupReports` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de agosto de 2021 a las 21:16 UTC
- Hora de edición: 10 de marzo de 2023 a las 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRolePolicyForBackupRestoreTesting

Descripción: esta política contiene permisos para probar las restauraciones y para limpiar los recursos creados durante las pruebas.

`AWSServiceRolePolicyForBackupRestoreTesting` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de noviembre de 2023 a las 23:37 UTC
- Hora de edición: 14 de febrero de 2024 a las 22:42 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSServiceRolePolicyForWorkspacesInstances

Descripción: Esta política gestionada proporciona acceso administrativo a Amazon WorkSpaces para gestionar EC2 las instancias en su Cuenta de AWS

`AWSServiceRolePolicyForWorkspacesInstances` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 11 de junio de 2025 a las 20:37 UTC
- Hora editada: 11 de junio de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSShieldDRTAccessPolicy

Descripción: Proporciona al equipo de respuesta AWS DDo S acceso limitado a usted para ayudarlo Cuenta de AWS a mitigar DDo los ataques S durante un evento de alta gravedad.

`AWSShieldDRTAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSShieldDRTAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 5 de junio de 2018 a las 22:29 UTC
- Hora de edición: 15 de diciembre de 2020 a las 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSShieldServiceRolePolicy

Descripción: Permite que AWS Shield acceda a AWS los recursos en su nombre para brindar protección DDo S.

`AWSShieldServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2021 a las 19:17 UTC
- Hora de edición: 17 de noviembre de 2021 a las 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSocialMessagingServiceRolePolicy

Descripción: proporciona acceso para publicar métricas y proporcionar información para el envío de mensajes de redes sociales.

`AWSSocialMessagingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de octubre de 2024 a las 19:28 h UTC
- Hora de edición: 10 de octubre de 2024 a las 19:28 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSMForSAPServiceLinkedRolePolicy

Descripción: Proporciona a AWS Systems Manager for SAP los permisos necesarios para gestionar e integrar el software de SAP con AWS.

`AWSSSMForSAPServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de noviembre de 2022 a las 01:18 UTC
- Hora editada: 8 de julio de 2025 a las 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v12 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSMOpsInsightsServiceRolePolicy

Descripción: Política para el rol vinculado al servicio AWSServiceRoleForAmazonSSM_OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de junio de 2021 a las 20:12 UTC
- Hora de edición: 16 de junio de 2021 a las 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSODirectoryAdministrator

Descripción: acceso de administrador para el Directorio de SSO

`AWSSSODirectoryAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSSODirectoryAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 31 de octubre de 2018 a las 23:54 UTC
- Hora de edición: 20 de octubre de 2022 a las 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSODirectoryReadOnly

Descripción: ReadOnly acceso al directorio SSO

`AWSSSODirectoryReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSSODirectoryReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 31 de octubre de 2018 a las 23:49 UTC
- Hora de edición: 16 de noviembre de 2022 a las 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSOMasterAccountAdministrator

Descripción: Proporciona acceso dentro del AWS SSO para gestionar AWS las cuentas maestras y miembros de Organizations y la aplicación en la nube

`AWSSSOMasterAccountAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSSOMasterAccountAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2018 a las 20:36 UTC
- Hora de edición: 26 de septiembre de 2024 a las 17:13 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSOMemberAccountAdministrator

Descripción: Proporciona acceso dentro del AWS SSO para administrar AWS las cuentas de los miembros de Organizations y la aplicación en la nube

`AWSSSOMemberAccountAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSSOMemberAccountAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2018 a las 20:45 UTC
- Hora de edición: 26 de abril de 2024 a las 00:31 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSOReadOnly

Descripción: Proporciona acceso de solo lectura a las configuraciones AWS de SSO.

`AWSSSOReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSSOReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de junio de 2018 a las 20:24 UTC
- Hora de edición: 26 de abril de 2024 a las 00:44 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSSOServiceRolePolicy

Descripción: Otorga permisos de inicio de sesión único AWS para administrar AWS los recursos, incluidas las funciones de IAM, las políticas y el IdP de SAML en su nombre.

`AWSSSOServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 5 de diciembre de 2017 a las 18:36 UTC
- Hora de edición: 11 de febrero de 2025 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Versión de la política

Versión de la política: v18 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStepFunctionsConsoleFullAccess

Descripción: política de acceso para proporcionar user/role/etc acceso a la AWS StepFunctions consola. Para disfrutar de una experiencia de consola completa, además de esta política, es posible que el usuario necesite el PassRole permiso iam: para desempeñar otras funciones de IAM que el servicio pueda asumir.

`AWSStepFunctionsConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSStepFunctionsConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 11 de enero de 2017 a las 21:54 UTC
- Hora de edición: 12 de enero de 2017 a las 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStepFunctionsFullAccess

Descripción: política de acceso para proporcionar user/role/etc acceso a la AWS StepFunctions API. Para tener acceso completo, además de esta política, el usuario DEBE tener el PassRole permiso iam: en al menos una función de IAM que pueda asumir el servicio.

`AWSStepFunctionsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSStepFunctionsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 11 de enero de 2017 a las 21:51 UTC
- Hora de edición: 11 de enero de 2017 a las 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStepFunctionsReadOnlyAccess

Descripción: política de acceso para proporcionar un acceso de solo user/role/etc lectura al AWS StepFunctions servicio.

`AWSStepFunctionsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSStepFunctionsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de enero de 2017 a las 21:46 UTC
- Hora de edición: 26 de abril de 2024 a las 18:53 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStorageGatewayFullAccess

Descripción: Proporciona acceso completo a AWS Storage Gateway a través de AWS Management Console.

`AWSStorageGatewayFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSStorageGatewayFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de septiembre de 2022 a las 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStorageGatewayReadOnlyAccess

Descripción: Proporciona acceso a AWS Storage Gateway a través de AWS Management Console.

`AWSStorageGatewayReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSStorageGatewayReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de septiembre de 2022 a las 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSStorageGatewayServiceRolePolicy

Descripción: Función vinculada al servicio que utiliza AWS Storage Gateway para permitir la integración de otros AWS servicios con Storage Gateway.

`AWSStorageGatewayServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2021 a las 19:03 UTC
- Hora de edición: 17 de febrero de 2021 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupplyChainFederationAdminAccess

Descripción: AWSSupply ChainFederationAdminAccess proporciona a los usuarios federados de AWS Supply Chain acceso a la aplicación AWS Supply Chain, incluidos los permisos necesarios para realizar acciones dentro de la aplicación AWS Supply Chain. La política proporciona permisos administrativos a los usuarios y grupos del Centro de Identidad de IAM y está asociada a un rol creado por AWS Supply Chain en su nombre. No debe adjuntar la AWSSupply ChainFederationAdminAccess política a ninguna otra entidad de IAM.

`AWSSupplyChainFederationAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupplyChainFederationAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de marzo de 2023 a las 18:54 UTC
- Hora editada: 11 de diciembre de 2024 a las 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportAccess

Descripción: Permite a los usuarios acceder al AWS Support Centro.

`AWSSupportAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupportAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportAppFullAccess

Descripción: Proporciona acceso completo a la AWS Support aplicación y a otros servicios necesarios, como AWS Support Service Quotas. Esta política incluye permisos para usar los servicios de soporte, de modo que el usuario pueda ponerse en contacto con AWS Support ellos en caso de asistencia, cambiar las cuotas de servicio y crear las funciones pertinentes vinculadas al servicio.

`AWSSupportAppFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupportAppFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de agosto de 2022 a las 16:53 UTC
- Hora de edición: 22 de agosto de 2022 a las 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportAppReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la AWS Support aplicación.

`AWSSupportAppReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupportAppReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 22 de agosto de 2022 a las 17:01 UTC
- Hora de edición: 22 de agosto de 2022 a las 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportPlansFullAccess

Descripción: proporciona acceso completo a los planes de soporte.

`AWSSupportPlansFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupportPlansFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de septiembre de 2022 a las 18:19 UTC
- Hora de edición: 09 de septiembre de 2024 a las 21:15 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportPlansReadOnlyAccess

Descripción: proporciona acceso de solo lectura a los planes de soporte.

`AWSSupportPlansReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSupportPlansReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de septiembre de 2022 a las 18:08 UTC
- Hora de edición: 09 de septiembre de 2024 a las 21:21 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSupportServiceRolePolicy

Descripción: Permite acceder AWS Support a AWS los recursos para proporcionar servicios de facturación, administrativos y de soporte.

`AWSSupportServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de abril de 2018 a las 18:04 UTC
- Hora editada: 18 de junio de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Versión de la política

Versión de la política: v40 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "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",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "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",
        "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:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "aoss:batchGetCollection",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "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: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:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
```

```
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "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",
        "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:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "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",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:listJobs",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentVersion",
        "bedrock:getCustomModel",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "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",
        "braket:getDevice",
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "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:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
```

```
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "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:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "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: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: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",
        "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: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:selectResourceConfig",
        "connect:describeContact",
        "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:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "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:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "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:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
```

```
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
        "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: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: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:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
```

```
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "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:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "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:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "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:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
```

```
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "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"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Action" : [
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "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: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: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",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "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",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegmentReferences",
        "evidently:listSegments",
```

```
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getExperiment",
        "fis:getExperimentTemplate",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "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: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",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
```

```
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "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:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "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:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTables",
        "glue:getTableVersions",
        "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:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:querySchemaVersionMetadata",
```

```
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "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:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "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: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: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: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:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "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",
        "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: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",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "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:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
```

```
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "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:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "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",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
```

```
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics: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",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "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",
        "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",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "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: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"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
```

```
      "Action" : [
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getOciOnboardingStatus",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "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:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listPoliciesForTarget",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
```

```
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
```

```
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "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:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "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:describeEvents",
```

```
        "rds:describeEventSubscriptions",
        "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: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: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",
        "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: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",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "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: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:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "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:describeMlflowTrackingServer",
        "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: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: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:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "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",
```

```
        "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",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "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: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",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
```

```
        "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:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "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:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "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",
        "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",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "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: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:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "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: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"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerAccountDiscoveryServicePolicy

Descripción: Concede permiso a AWS Systems Manager (SSM) para descubrir Cuenta de AWS información.

`AWSSystemsManagerAccountDiscoveryServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de octubre de 2019 a las 17:21 UTC
- Hora de edición: 17 de octubre de 2022 a las 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerChangeManagementServicePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por el marco de gestión de cambios de AWS Systems Manager.

`AWSSystemsManagerChangeManagementServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 7 de diciembre de 2020 a las 22:21 UTC
- Hora de edición: 7 de diciembre de 2020 a las 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Descripción: Proporciona permisos para que AWS Systems Manager Quick Setup habilite y configure el registro de la configuración de AWS Config.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:40 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:40 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerEnableExplorerExecutionPolicy

Descripción: Esta política concede permisos administrativos para activar Explorer, una función de AWS Systems Manager. Esto incluye permisos para actualizar la configuración de servicio relacionada de Systems Manager y para crear un rol vinculado al servicio para Systems Manager.

`AWSSystemsManagerEnableExplorerExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerEnableExplorerExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de junio de 2024 a las 09:42 h UTC
- Hora de edición: 26 de junio de 2024 a las 09:42 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerForSAPFullAccess

Descripción: Proporciona acceso completo al servicio AWS Systems Manager for SAP

`AWSSystemsManagerForSAPFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerForSAPFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2022 a las 02:11 UTC
- Hora de edición: 10 de julio de 2024 a las 21:54 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerForSAPReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al servicio AWS Systems Manager for SAP

`AWSSystemsManagerForSAPReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerForSAPReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de noviembre de 2022 a las 02:11 UTC
- Hora de edición: 17 de noviembre de 2022 a las 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerJustInTimeAccessServicePolicy

Descripción: Proporciona acceso a AWS los recursos gestionados o utilizados por el marco de acceso justo a tiempo de AWS Systems Manager.

`AWSSystemsManagerJustInTimeAccessServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de abril de 2025 a las 20:07 UTC
- Hora editada: 21 de abril de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerJustInTimeAccessTokenPolicy

Descripción: La política gestionada AWSSystems ManagerJustInTimeAccessTokenPolicy permite a Systems Manager generar tokens de acceso que se utilizan para el acceso a los just-in-time nodos.

`AWSSystemsManagerJustInTimeAccessTokenPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerJustInTimeAccessTokenPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de abril de 2025 a las 21:07 UTC
- Hora editada: 17 de abril de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "TerminateAndResumeSession",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Descripción: La política administrada AWSSystems ManagerJustInTimeAccessTokenSessionPolicy permite a Systems Manager aplicar permisos restringidos a una sesión de acceso a un just-in-time nodo una vez iniciada.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 17 de abril de 2025 a las 20:52 UTC

- Hora editada: 17 de abril de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Descripción: Esta política permite a Systems Manager compartir una política de denegación de acceso para el acceso a los just-in-time nodos desde la cuenta del administrador delegado a las cuentas de los miembros y replicar la política en varias regiones.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 21 de abril de 2025 a las 20:52 UTC
- Hora editada: 23 de abril de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerNotificationsServicePolicy

Descripción: Permisos necesarios para recopilar información sobre un usuario para las notificaciones Just-In-Time-Node de -Access.

`AWSSystemsManagerNotificationsServicePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de abril de 2025 a las 20:52 UTC
- Hora editada: 17 de abril de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Descripción: función de IAM para que SSM Explorer gestione las operaciones relacionadas OpsData

`AWSSystemsManagerOpsDataSyncServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de abril de 2021 a las 20:42 UTC
- Hora de edición: 28 de junio de 2023 a las 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxAssetServerPolicy

Descripción: Esta política concede al AWS Portal Asset Server los permisos necesarios para su funcionamiento normal.

`AWSThinkboxAssetServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxAssetServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:18 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
```

```
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxAWSPortalAdminPolicy

Descripción: Esta política otorga al software Deadline de AWS Thinkbox acceso completo a varios AWS servicios necesarios para la administración AWS del Portal. Esto incluye el acceso para crear etiquetas arbitrarias en varios tipos EC2 de recursos.

`AWSThinkboxAWSPortalAdminPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxAWSPortalAdminPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:41 UTC
- Hora editada: 12 de noviembre de 2024 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    },
    {
      "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*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxAWSPortalGatewayPolicy

Descripción: Esta política concede al equipo de AWS Portal Gateway los permisos necesarios para su funcionamiento normal.

`AWSThinkboxAWSPortalGatewayPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxAWSPortalGatewayPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:05 UTC
- Hora de edición: 30 de junio de 2020 a las 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxAWSPortalWorkerPolicy

Descripción: Esta política otorga a los trabajadores de Deadline Workers del AWS Portal los permisos necesarios para su funcionamiento normal.

`AWSThinkboxAWSPortalWorkerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxAWSPortalWorkerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:15 UTC
- Hora de edición: 7 de diciembre de 2020 a las 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Descripción: Otorga los permisos necesarios para el funcionamiento del rastreador de recursos de fecha límite de AWS Thinkbox. Esto incluye el acceso completo a algunas EC2 acciones, como DeleteFleets y CancelSpotFleetRequests.

`AWSThinkboxDeadlineResourceTrackerAccessPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxDeadlineResourceTrackerAccessPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:25 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Descripción: Otorga los permisos necesarios para crear, destruir y administrar el Deadline Resource Tracker de AWS Thinkbox.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxDeadlineResourceTrackerAdminPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:29 UTC
- Hora editada: 12 de noviembre de 2024 a las 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Descripción: Otorga los permisos necesarios para el complemento Deadline Spot Event de AWS Thinkbox. Esto incluye el permiso para solicitar, modificar y cancelar una flota de spots, así como el PassRole permiso limitado.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:38 UTC
- Hora de edición: 27 de mayo de 2020 a las 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Descripción: Concede los permisos necesarios para una EC2 instancia que ejecute el software AWS Thinkbox Deadline Spot Event Plugin Worker.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de mayo de 2020 a las 19:35 UTC
- Hora de edición: 7 de diciembre de 2020 a las 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTransferConsoleFullAccess

Descripción: Proporciona acceso completo a AWS Transfer a través del AWS Management Console

`AWSTransferConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTransferConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de diciembre de 2020 a las 19:33 UTC
- Hora de edición: 14 de diciembre de 2020 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTransferFullAccess

Descripción: Proporciona acceso completo al servicio AWS de transferencia.

`AWSTransferFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTransferFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de diciembre de 2020 a las 19:37 UTC
- Hora de edición: 14 de diciembre de 2020 a las 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTransferLoggingAccess

Descripción: Permite a AWS Transfer tener acceso completo para crear grupos y flujos de registro y guardar los eventos de registro en su cuenta

`AWSTransferLoggingAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTransferLoggingAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de enero de 2019 a las 15:32 UTC
- Hora de edición: 14 de enero de 2019 a las 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTransferReadOnlyAccess

Descripción: Proporcione acceso de solo lectura a los servicios AWS de transferencia.

`AWSTransferReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTransferReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de agosto de 2020 a las 17:54 UTC
- Hora de edición: 27 de agosto de 2020 a las 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTrustedAdvisorPriorityFullAccess

Descripción: Proporciona acceso completo a AWS Trusted Advisor Priority. Esta política también permite al usuario añadir Trusted Advisor como un servicio de confianza en AWS Organizations y especificar cuentas de administrador delegado para Trusted Advisor Priority.

`AWSTrustedAdvisorPriorityFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTrustedAdvisorPriorityFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de agosto de 2022 a las 16:08 UTC
- Hora de edición: 16 de agosto de 2022 a las 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTrustedAdvisorPriorityReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS Trusted Advisor Priority. Esto incluye el permiso para ver las cuentas de administrador delegadas.

`AWSTrustedAdvisorPriorityReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSTrustedAdvisorPriorityReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 16 de agosto de 2022 a las 16:35 UTC
- Hora de edición: 16 de agosto de 2022 a las 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
```

```
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTrustedAdvisorReportingServiceRolePolicy

Descripción: política de servicio para la generación de informes de múltiples cuentas de Trusted Advisor

`AWSTrustedAdvisorReportingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de noviembre de 2019 a las 17:41 UTC
- Hora de edición: 28 de febrero de 2023 a las 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSTrustedAdvisorServiceRolePolicy

Descripción: Acceso al servicio AWS Trusted Advisor para ayudar a reducir los costos, aumentar el rendimiento y mejorar la seguridad de su AWS entorno.

`AWSTrustedAdvisorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de febrero de 2018 a las 21:24 UTC
- Hora editada: 30 de octubre de 2024 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSUserNotificationsServiceLinkedRolePolicy

Descripción: Permite que las notificaciones de AWS usuario llamen a AWS los servicios en su nombre.

`AWSUserNotificationsServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de abril de 2023 a las 13:28 UTC
- Hora editada: 14 de enero de 2025 a las 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVendorInsightsAssessorFullAccess

Descripción: proporciona acceso completo para ver los recursos titulados de Información de proveedores y administrar las suscripciones a Información de proveedores

`AWSVendorInsightsAssessorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSVendorInsightsAssessorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVendorInsightsAssessorReadOnly

Descripción: proporciona acceso de solo lectura para ver los recursos autorizados de Información de proveedores

`AWSVendorInsightsAssessorReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSVendorInsightsAssessorReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVendorInsightsVendorFullAccess

Descripción: proporciona acceso completo para crear y administrar los recursos de Información de proveedores

`AWSVendorInsightsVendorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSVendorInsightsVendorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 19 de octubre de 2023 a las 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVendorInsightsVendorReadOnly

Descripción: proporciona acceso de solo lectura para ver los recursos de Información de proveedores

`AWSVendorInsightsVendorReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSVendorInsightsVendorReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 26 de julio de 2022 a las 15:05 UTC
- Hora de edición: 1 de diciembre de 2022 a las 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVpcLatticeServiceRolePolicy

Descripción: Permite que VPC Lattice acceda a AWS los recursos en su nombre.

`AWSVpcLatticeServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2022 a las 20:47 UTC
- Hora editada: 1 de diciembre de 2024 a las 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVPCS2SVpnServiceRolePolicy

Descripción: Permita que la Site-to-Site VPN cree y administre los recursos relacionados con sus conexiones VPN.

`AWSVPCS2SVpnServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de agosto de 2019 a las 14:13 UTC
- Hora editada: 15 de mayo de 2025 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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!*"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVPCTransitGatewayServiceRolePolicy

Descripción: permite que la Puerta de enlace de tránsito de la VPC cree y administre los recursos necesarios para las conexiones de VPC de a Puerta de enlace tránsito.

`AWSVPCTransitGatewayServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2018 a las 16:21 UTC
- Hora de edición: 15 de abril de 2021 a las 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSVPCVerifiedAccessServiceRolePolicy

Descripción: Política para permitir que el servicio de acceso AWS verificado aprovisione puntos de conexión en su nombre

`AWSVPCVerifiedAccessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2022 a las 03:35 UTC
- Hora de edición: 17 de noviembre de 2023 a las 21:03 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWAFConsoleFullAccess

Descripción: Proporciona acceso completo a AWS WAF a través del AWS Management Console. Tenga en cuenta que esta política también otorga permisos para publicar y actualizar CloudFront las distribuciones de Amazon, permisos para ver los balanceadores de carga en AWS Elastic Load Balancing, permisos para ver las etapas APIs y REST de Amazon API Gateway, permisos para enumerar y ver CloudWatch las métricas de Amazon y permisos para ver las regiones habilitadas en la cuenta.

`AWSWAFConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSWAFConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 6 de abril de 2020 a las 18:38 UTC
- Hora editada: 5 de mayo de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
```

```
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis"
      ],
      "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" : "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"
          ]
        }
      }
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWAFConsoleReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a AWS WAF a través del. AWS Management Console Tenga en cuenta que esta política también otorga permisos para publicar CloudFront distribuciones de Amazon, permisos para ver los balanceadores de carga en AWS Elastic Load Balancing, permisos para ver las etapas APIs y REST de Amazon API Gateway, permisos para enumerar y ver CloudWatch las métricas de Amazon y permisos para ver las regiones habilitadas en la cuenta.

`AWSWAFConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSWAFConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 6 de abril de 2020 a las 18:43 UTC
- Hora editada: 5 de mayo de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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" : "AllowListActionsForALB",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis"
      ],
      "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" : "*"
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWAFFullAccess

Descripción: Proporciona acceso completo a las acciones AWS del WAF.

`AWSWAFFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSWAFFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de octubre de 2015 a las 20:44 UTC
- Hora editada: 5 de mayo de 2025 a las 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Versión de la política

Versión de la política: v12 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
```

```
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "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" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWAFReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a las acciones de AWS WAF.

`AWSWAFReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSWAFReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de octubre de 2015 a las 20:43 UTC
- Hora editada: 5 de mayo de 2025 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWellArchitectedDiscoveryServiceRolePolicy

Descripción: Permite acceder WellArchitected a AWS los servicios y recursos relacionados con WellArchitected los recursos en nombre de los clientes.

`AWSWellArchitectedDiscoveryServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de abril de 2023 a las 18:36 UTC
- Hora de edición: 26 de abril de 2023 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWellArchitectedOrganizationsServiceRolePolicy

Descripción: permite que Well-Architected acceda a Organizations en su nombre.

`AWSWellArchitectedOrganizationsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de junio de 2022 a las 17:15 UTC
- Hora de edición: 25 de julio de 2022 a las 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSWickrFullAccess

Descripción: esta política concede permisos administrativos completos al servicio de Wickr, incluidas las funciones administrativas de Wickr bajo la AWS Management Console.

`AWSWickrFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSWickrFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 20:36 UTC
- Hora de edición: 27 de noviembre de 2022 a las 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSXrayCrossAccountSharingConfiguration

Descripción: proporciona capacidades para administrar los enlaces de Observability Access Manager y establecer el intercambio de trazas de X-Ray

`AWSXrayCrossAccountSharingConfiguration` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSXrayCrossAccountSharingConfiguration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 13:46 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSXRayDaemonWriteAccess

Descripción: Permita que AWS X-Ray Daemon transmita datos de segmentos de rastreo sin procesar a la API del servicio y recupere datos de muestreo (reglas, objetivos, etc.) para que los utilice el SDK de X-Ray.

`AWSXRayDaemonWriteAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSXRayDaemonWriteAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de agosto de 2018 a las 23:00 UTC
- Hora de edición: 13 de febrero de 2024 a las 21:58 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSXrayFullAccess

Descripción: Política gestionada de acceso completo de AWS X-Ray

`AWSXrayFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSXrayFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 18:30 UTC
- Hora de edición: 11 de abril de 2024 a las 17:07 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSXrayReadOnlyAccess

Descripción: Política gestionada de solo lectura de AWS X-Ray

`AWSXrayReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSXrayReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 18:27 UTC
- Hora de edición: 14 de febrero de 2024 a las 00:35 h UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSXrayWriteOnlyAccess

Descripción: Política gestionada solo por AWS X-Ray

`AWSXrayWriteOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `AWSXrayWriteOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2016 a las 18:19 UTC
- Hora de edición: 28 de agosto de 2018 a las 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSZonalAutoshiftPracticeRunSLRPolicy

Descripción: Proporciona acceso administrativo a las prácticas de turno zonal del ARC y acceso a los estados de CloudWatch alarma para monitorear las prácticas de turno.

`AWSZonalAutoshiftPracticeRunSLRPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2023 a las 17:34 h UTC
- Hora editada: 30 de junio de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

AWSZoneGroupAccessManagementServiceRolePolicy

Descripción: Proporciona acceso de solo lectura a lo APIs necesario para facilitar la administración del acceso a los grupos de zonas para las organizaciones.

`AWSZoneGroupAccessManagementServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de julio de 2025 a las 19:07 UTC
- Hora editada: 1 de julio de 2025 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

BatchServiceRolePolicy

Descripción: Proporciona acceso al servicio AWS Batch para gestionar los recursos necesarios, incluidos los recursos de Amazon EC2 y Amazon ECS.

`BatchServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de marzo de 2021 a las 06:55 UTC
- Hora de edición: 05 de diciembre de 2023 a las 22:52 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Billing

Descripción: concede permisos para administrar la facturación y los costos. Esto incluye ver el uso de la cuenta, modificar los presupuestos y los métodos de pago.

`Billing` es una política administrada de AWS.

Uso de la política

Puede asociar `Billing` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:33 UTC
- Hora editada: 12 de marzo de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Versión de la política

Versión de la política: v15 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:ListTagsForResource",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CertificateManagerServiceRolePolicy

Descripción: política de rol de servicio de Amazon Certificate Manager

`CertificateManagerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de junio de 2020 a las 17:56 UTC
- Hora de edición: 25 de junio de 2020 a las 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ClientVPNServiceConnectionsRolePolicy

Descripción: Política para permitir que AWS Client VPN administre sus conexiones de punto final de Client VPN.

`ClientVPNServiceConnectionsRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de agosto de 2020 a las 19:48 UTC

- Hora de edición: 12 de agosto de 2020 a las 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ClientVPNServiceRolePolicy

Descripción: Política para permitir que AWS Client VPN administre sus puntos finales de Client VPN.

`ClientVPNServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de diciembre de 2018 a las 21:20 UTC
- Hora de edición: 12 de agosto de 2020 a las 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudFormationStackSetsOrgAdminServiceRolePolicy

Descripción: Función de servicio para CloudFormation StackSets (cuenta maestra de la organización)

`CloudFormationStackSetsOrgAdminServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de diciembre de 2019 a las 00:20 UTC

- Hora de edición: 10 de diciembre de 2019 a las 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudFormationStackSetsOrgMemberServiceRolePolicy

Descripción: Función de servicio para CloudFormation StackSets (cuenta de miembro de la organización)

`CloudFormationStackSetsOrgMemberServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de diciembre de 2019 a las 23:52 UTC
- Hora de edición: 9 de diciembre de 2019 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudFrontFullAccess

Descripción: Proporciona acceso completo a la CloudFront consola, además de la posibilidad de enumerar los buckets de Amazon S3 a través del AWS Management Console.

`CloudFrontFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudFrontFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 28 de abril de 2025 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
```

```
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Sid" : "cfrequestcertificate",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudFrontReadOnlyAccess

Descripción: Proporciona acceso a la información CloudFront de configuración de la distribución y enumera las distribuciones a través del AWS Management Console.

`CloudFrontReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudFrontReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 28 de abril de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudHSMServiceRolePolicy

Descripción: Permite el acceso a AWS los recursos utilizados o gestionados por CloudHSM

`CloudHSMServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 6 de noviembre de 2017 a las 19:12 UTC
- Hora de edición: 6 de noviembre de 2017 a las 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudSearchFullAccess

Descripción: Proporciona acceso completo al servicio de CloudSearch configuración de Amazon.

`CloudSearchFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudSearchFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudSearchReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al servicio de CloudSearch configuración de Amazon.

`CloudSearchReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudSearchReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudTrailEventContext

Descripción: Este rol vinculado al servicio permite CloudTrail obtener y agregar etiquetas de recursos a los CloudTrail eventos del propietario del recurso.

`CloudTrailEventContext` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de mayo de 2025 a las 13:52 UTC
- Hora editada: 15 de mayo de 2025 a las 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudTrailServiceRolePolicy

Descripción: Política de permisos para CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de octubre de 2018 a las 21:21 UTC
- Hora de edición: 27 de noviembre de 2023 a las 01:18 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatch-CrossAccountAccess

Descripción: Permite CloudWatch asumir CloudWatch CrossAccountSharing funciones en cuentas remotas en nombre de la cuenta corriente para mostrar datos entre cuentas y regiones

`CloudWatch-CrossAccountAccess` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de julio de 2019 a las 09:59 UTC
- Hora de edición: 23 de julio de 2019 a las 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
```

```
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchActionsEC2Access

Descripción: Proporciona acceso de solo lectura a CloudWatch las alarmas y las métricas, así como EC2 a los metadatos. Proporciona acceso a las instancias de detención, finalización y reinicio EC2 .

`CloudWatchActionsEC2Access` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchActionsEC2Access` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de julio de 2015 a las 00:00 UTC
- Hora de edición: 7 de julio de 2015 a las 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchAgentAdminPolicy

Descripción: Se requieren todos los permisos para su uso AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchAgentAdminPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de marzo de 2018 a las 00:52 UTC
- Hora de edición: 05 de febrero de 2024 a las 20:59 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchAgentServerPolicy

Descripción: Se requieren permisos para su uso AmazonCloudWatchAgent en los servidores

`CloudWatchAgentServerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchAgentServerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de marzo de 2018 a las 01:06 UTC
- Hora de edición: 06 de febrero de 2024 a las 16:37 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchApplicationInsightsFullAccess

Descripción: Proporciona acceso completo a CloudWatch Application Insights y a las dependencias necesarias.

`CloudWatchApplicationInsightsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchApplicationInsightsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de noviembre de 2020 a las 18:44 UTC
- Hora de edición: 25 de enero de 2022 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchApplicationInsightsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a CloudWatch Application Insights.

`CloudWatchApplicationInsightsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchApplicationInsightsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de noviembre de 2020 a las 18:48 UTC
- Hora de edición: 24 de noviembre de 2020 a las 18:48 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Descripción: política de rol vinculada al servicio de Información de aplicaciones de CloudWatch

`CloudwatchApplicationInsightsServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2018 a las 16:22 UTC
- Hora de edición: 25 de julio de 2024 a las 16:24 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v25 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
```

```
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchApplicationSignalsFullAccess

Descripción: Proporcione acceso completo al servicio CloudWatch Application Signals y acceso limitado a las dependencias necesarias para usar y operar este servicio.

`CloudWatchApplicationSignalsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchApplicationSignalsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 06 de junio de 2024 a las 22:50 h UTC
- Hora de edición: 06 de junio de 2024 a las 22:50 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "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" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : "xray:GetTraceSummaries",
      "Resource" : "*"
    },
    {
      "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchApplicationSignalsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura al servicio CloudWatch Application Signals y acceso limitado a las dependencias necesarias para utilizar este servicio

`CloudWatchApplicationSignalsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchApplicationSignalsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 06 de junio de 2024 a las 22:48 h UTC
- Hora de edición: 06 de junio de 2024 a las 22:48 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "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" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchApplicationSignalsServiceRolePolicy

Descripción: La política otorga permiso a CloudWatch Application Signals para recopilar datos de monitoreo y etiquetado de otros AWS servicios relevantes.

`CloudWatchApplicationSignalsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2023 a las 18:09 UTC
- Hora de edición: 17 de marzo de 2025 a las 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchAutomaticDashboardsAccess

Descripción: Proporciona acceso a los paneles CloudWatch automáticos que no CloudWatch APIs se utilizan para mostrar, incluido el contenido de los objetos, como las funciones de Lambda

`CloudWatchAutomaticDashboardsAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchAutomaticDashboardsAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 23 de julio de 2019 a las 10:01 UTC
- Hora de edición: 20 de abril de 2021 a las 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchCrossAccountSharingConfiguration

Descripción: Proporciona capacidades para administrar los enlaces de Observability Access Manager y establecer el uso compartido de CloudWatch recursos

`CloudWatchCrossAccountSharingConfiguration` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchCrossAccountSharingConfiguration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 14:01 UTC
- Hora de edición: 27 de noviembre de 2022 a las 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchEventsBuiltInTargetExecutionAccess

Descripción: Permite que los objetivos integrados en Amazon CloudWatch Events realicen EC2 acciones en su nombre.

`CloudWatchEventsBuiltInTargetExecutionAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchEventsBuiltInTargetExecutionAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de enero de 2016 a las 18:35 UTC
- Hora de edición: 14 de enero de 2016 a las 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchEventsFullAccess

Descripción: Proporciona acceso completo a Amazon CloudWatch Events.

`CloudWatchEventsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchEventsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de enero de 2016 a las 18:37 UTC
- Hora editada: 22 de enero de 2025 a las 02:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchEventsInvocationAccess

Descripción: Permite a Amazon CloudWatch Events retransmitir eventos a las transmisiones de AWS Kinesis Streams de su cuenta.

`CloudWatchEventsInvocationAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchEventsInvocationAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de enero de 2016 a las 18:36 UTC
- Hora de edición: 14 de enero de 2016 a las 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchEventsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon CloudWatch Events.

`CloudWatchEventsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchEventsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 14 de enero de 2016 a las 18:27 UTC

- Hora de edición: 1 de diciembre de 2022 a las 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchEventsServiceRolePolicy

Descripción: Permite AWS CloudWatch ejecutar acciones en su nombre configuradas mediante alarmas y eventos.

`CloudWatchEventsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de noviembre de 2017 a las 00:42 UTC
- Hora de edición: 17 de noviembre de 2017 a las 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchFullAccess

Descripción: Proporciona acceso completo a CloudWatch.

`CloudWatchFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchFullAccessV2

Descripción: Proporciona acceso completo a CloudWatch.

`CloudWatchFullAccessV2` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchFullAccessV2` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de agosto de 2023 a las 11:32 UTC
- Hora de edición: 17 de mayo de 2024 a las 22:20 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchInternetMonitorFullAccess

Descripción: proporciona acceso completo a las acciones para trabajar con Amazon CloudWatch Internet Monitor. También proporciona acceso a otros servicios, como Amazon CloudWatch, Amazon EC2 CloudFront, Amazon WorkSpaces y Elastic Load Balancing, que son necesarios para utilizar el servicio Internet Monitor para supervisar y almacenar información sobre el tráfico de aplicaciones.

`CloudWatchInternetMonitorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchInternetMonitorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de octubre de 2024 a las 21:02 h UTC
- Hora de edición: 22 de octubre de 2024 a las 21:02 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchInternetMonitorReadOnlyAccess

Descripción: proporciona acceso de solo lectura a las acciones para trabajar con Amazon CloudWatch Internet Monitor. También proporciona acceso a otros servicios de Amazon CloudWatch, incluidas las políticas para recuperar información sobre las CloudWatch métricas y gestionar las consultas de registro, que son necesarias para utilizar el servicio Internet Monitor para supervisar y almacenar información sobre el tráfico de las aplicaciones.

`CloudWatchInternetMonitorReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchInternetMonitorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de noviembre de 2024 a las 23:11 UTC
- Hora editada: 12 de noviembre de 2024 a las 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchInternetMonitorServiceRolePolicy

Descripción: Permite que Internet Monitor acceda a los espacios de trabajo EC2, CloudFront los recursos y otros servicios necesarios en su nombre.

`CloudWatchInternetMonitorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 27 de noviembre de 2022 a las 17:46 UTC
- Hora de edición: 20 de julio de 2023 a las 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Descripción: Proporciona acceso de escritura al grupo de registros de X-Ray y CloudWatch Application Signals.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de octubre de 2024 a las 19:09 h UTC
- Hora de edición: 16 de octubre de 2024 a las 19:09 h UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchLambdaInsightsExecutionRolePolicy

Descripción: política requerida para la extensión de Lambda Insights

`CloudWatchLambdaInsightsExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchLambdaInsightsExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 7 de octubre de 2020 a las 19:27 UTC
- Hora de edición: 7 de octubre de 2020 a las 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchLogsCrossAccountSharingConfiguration

Descripción: Proporciona capacidades para administrar los enlaces de Observability Access Manager y establecer el uso compartido de los recursos de CloudWatch Logs

`CloudWatchLogsCrossAccountSharingConfiguration` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchLogsCrossAccountSharingConfiguration` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 27 de noviembre de 2022 a las 13:55 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchLogsFullAccess

Descripción: Proporciona acceso completo a los CloudWatch registros

`CloudWatchLogsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchLogsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 20 de mayo de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchLogsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a CloudWatch los registros

`CloudWatchLogsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchLogsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 20 de mayo de 2025 a las 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Versión de la política

Versión de la política: v7 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Descripción: Puede utilizar esta política en las funciones de IAM asociadas a los recursos de instancia de Amazon EC2 y Amazon EKS para enviar informes de telemetría (métricas) a un punto final de Network Flow Monitor.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchNetworkFlowMonitorAgentPublishPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 1 de diciembre de 2024 a las 22:51 UTC
- Hora editada: 1 de diciembre de 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchNetworkFlowMonitorServiceRolePolicy

Descripción: No puedes asociarte CloudWatchNetworkFlowMonitorServiceRolePolicy a tus entidades de IAM. Esta política está asociada a un rol vinculado a un servicio denominado AWSServiceRoleForNetworkFlowMonitor, que publica los resultados de agregación de telemetría de

red recopilados por los agentes de Network Flow Monitor para. CloudWatch También permite que el servicio utilice AWS Organizations para obtener información para escenarios de varias cuentas.

`CloudWatchNetworkFlowMonitorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2024 a las 22:36 UTC
- Hora editada: 29 de abril de 2025 a las 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Descripción: No puedes asociarte CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy a tus entidades de IAM. Esta política está asociada a un rol vinculado a un servicio denominado AWSServiceRoleForNetworkFlowMonitor_Topology, que genera instantáneas topológicas de los recursos utilizados por Network Flow Monitor en su cuenta.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 1 de diciembre de 2024 a las 22:51 UTC
- Hora editada: 1 de diciembre de 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchNetworkMonitorServiceRolePolicy

Descripción: Permite que CloudWatch Network Monitor acceda a los recursos de VPC EC2 y los administre, publique datos CloudWatch y acceda a otros servicios necesarios en su nombre.

`CloudWatchNetworkMonitorServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de diciembre de 2023 a las 18:53 h UTC
- Hora de edición: 21 de diciembre de 2023 a las 18:53 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchOpenSearchDashboardAccess

Descripción: Esta política proporciona a los usuarios acceso para ver los OpenSearch paneles en la consola de CloudWatch Logs.

`CloudWatchOpenSearchDashboardAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchOpenSearchDashboardAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2024 a las 21:06 UTC
- Hora editada: 1 de diciembre de 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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_*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchOpenSearchDashboardsFullAccess

Descripción: Esta política proporciona a los usuarios acceso a la consola de CloudWatch Logs OpenSearch para crear, actualizar, eliminar o ver los paneles de control.

`CloudWatchOpenSearchDashboardsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchOpenSearchDashboardsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2024 a las 21:06 UTC
- Hora editada: 1 de diciembre de 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a CloudWatch.

`CloudWatchReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora editada: 21 de noviembre de 2024 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Versión de la política

Versión de la política: v10 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*",
        "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",
        "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"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchSyntheticsFullAccess

Descripción: Proporciona acceso completo a CloudWatch Synthetics.

`CloudWatchSyntheticsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchSyntheticsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de noviembre de 2019 a las 17:39 UTC
- Hora editada: 21 de noviembre de 2024 a las 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CloudWatchSyntheticsReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CloudWatchSyntheticsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de noviembre de 2019 a las 17:45 UTC
- Hora de edición: 6 de marzo de 2020 a las 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComprehendDataAccessRolePolicy

Descripción: Política para la función de servicio AWS Comprehend que permite el acceso a los recursos de S3 para el acceso a los datos

`ComprehendDataAccessRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ComprehendDataAccessRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de marzo de 2019 a las 22:28 UTC
- Hora de edición: 6 de marzo de 2019 a las 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComprehendFullAccess

Descripción: proporciona acceso completo a Amazon Comprehend.

`ComprehendFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ComprehendFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 18:08 UTC
- Hora de edición: 5 de diciembre de 2017 a las 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComprehendMedicalFullAccess

Descripción: proporciona acceso completo a Amazon Comprehend Medical

`ComprehendMedicalFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ComprehendMedicalFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 17:55 UTC
- Hora de edición: 27 de noviembre de 2018 a las 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComprehendReadOnly

Descripción: proporciona acceso de solo lectura a Amazon Comprehend.

`ComprehendReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `ComprehendReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 18:10 UTC
- Hora de edición: 26 de abril de 2022 a las 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Versión de la política

Versión de la política: v11 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComputeOptimizerReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ComputeOptimizerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 7 de marzo de 2020 a las 00:11 UTC
- Hora editada: 20 de noviembre de 2024 a las 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Versión de la política

Versión de la política: v9 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ComputeOptimizerServiceRolePolicy

Descripción: Permite llamar ComputeOptimizer a AWS los servicios y recopilar detalles de la carga de trabajo en su nombre.

`ComputeOptimizerServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 3 de diciembre de 2019 a las 08:45 UTC
- Hora editada: 3 de enero de 2025 a las 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ConfigConformsServiceRolePolicy

Descripción: Política necesaria para AWSConfig crear paquetes de conformidad

`ConfigConformsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de julio de 2019 a las 21:38 UTC
- Hora de edición: 12 de enero de 2023 a las 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CostOptimizationHubAdminAccess

Descripción: esta política administrada proporciona acceso de administrador al Centro de optimización de costos.

`CostOptimizationHubAdminAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CostOptimizationHubAdminAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 19 de diciembre de 2023 a las 00:03 h UTC
- Hora de edición: 19 diciembre de 2023 a las 00:03 h UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CostOptimizationHubReadOnlyAccess

Descripción: esta política administrada proporciona acceso de solo lectura al Centro de optimización de costos.

`CostOptimizationHubReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `CostOptimizationHubReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de diciembre de 2023 a las 18:04 h UTC
- Hora de edición: 13 de diciembre de 2023 a las 18:04 h UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CostOptimizationHubServiceRolePolicy

Descripción: permite que el Centro de optimización de costos recupere información de la organización y recopile datos y metadatos relacionados con la optimización.

`CostOptimizationHubServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de noviembre de 2023 a las 08:03 h UTC
- Hora de edición: 05 de julio de 2024 a las 18:02 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

CustomerProfilesServiceLinkedRolePolicy

Descripción: Permite que los perfiles de clientes de Amazon Connect accedan a los AWS servicios y recursos en su nombre.

`CustomerProfilesServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de marzo de 2023 a las 22:56 UTC
- Hora editada: 26 de noviembre de 2024 a las 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DatabaseAdministrator

Descripción: Otorga permisos de acceso total a AWS los servicios y acciones necesarios para configurar y configurar los servicios AWS de bases de datos.

`DatabaseAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `DatabaseAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:25 UTC
- Hora de edición: 8 de enero de 2019 a las 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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"
      ]
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DataScientist

Descripción: Otorga permisos a los servicios AWS de análisis de datos.

`DataScientist` es una política administrada de AWS.

Uso de la política

Puede asociar `DataScientist` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:28 UTC
- Hora de edición: 3 de diciembre de 2019 a las 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DAXServiceRolePolicy

Descripción: esta política permite que DAX cree y administre la interfaz de red, el grupo de seguridad, la subred y la VPC en nombre del cliente

`DAXServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de marzo de 2018 a las 17:51 UTC
- Hora de edición: 5 de marzo de 2018 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DeclarativePoliciesEC2Report

Descripción: Proporciona acceso al informe de solo lectura APIs necesario para ejecutar el informe de estado de la cuenta de políticas EC2 declarativas.

`DeclarativePoliciesEC2Report` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 30 de noviembre de 2024 a las 13:21 UTC
- Hora editada: 30 de noviembre de 2024 a las 13:21 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Descripción: Se requieren permisos para admitir Amazon CloudWatch Contributor Insights para Amazon DynamoDB.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2019 a las 21:13 UTC
- Hora de edición: 15 de noviembre de 2019 a las 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DynamoDBKinesisReplicationServiceRolePolicy

Descripción: Proporcionar acceso a AWS DynamoDB a KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de noviembre de 2020 a las 00:43 UTC
- Hora de edición: 12 de noviembre de 2020 a las 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

DynamoDBReplicationServiceRolePolicy

Descripción: permisos requeridos por DynamoDB para la replicación de datos entre regiones

`DynamoDBReplicationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 9 de noviembre de 2017 a las 23:55 UTC
- Hora de edición: 08 de enero de 2024 a las 20:10 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2FastLaunchFullAccess

Descripción: Esta política otorga acceso completo a las acciones de EC2 Fast Launch

`EC2FastLaunchFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `EC2FastLaunchFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 13 de mayo de 2024 a las 22:45 h UTC
- Hora editada: 14 de mayo de 2025 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2FastLaunchServiceRolePolicy

Descripción: política que concede a ec2fastlaunch la capacidad de preparar y administrar las instantáneas aprovisionadas previamente en la cuenta del cliente y publicar las métricas relacionadas.

`EC2FastLaunchServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de enero de 2022 a las 13:08 UTC
- Hora editada: 14 de mayo de 2025 a las 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2FleetTimeShiftableServiceRolePolicy

Descripción: Política que otorga permisos a EC2 Fleet para lanzar instancias en el futuro.

`EC2FleetTimeShiftableServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 23 de diciembre de 2019 a las 19:47 UTC
- Hora de edición: 23 de diciembre de 2019 a las 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
        }
      }
    }
```

```
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Ec2ImageBuilderCrossAccountDistributionAccess

Descripción: EC2 Image Builder necesita permisos para realizar una distribución entre cuentas.

`Ec2ImageBuilderCrossAccountDistributionAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `Ec2ImageBuilderCrossAccountDistributionAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de septiembre de 2020 a las 19:22 UTC
- Hora de edición: 30 de septiembre de 2020 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2ImageBuilderLifecycleExecutionPolicy

Descripción: La EC2 ImageBuilderLifecycleExecutionPolicy política concede permisos para que Image Builder lleve a cabo acciones como desaprobar o eliminar los recursos de imagen de Image Builder y sus recursos subyacentes (AMIsinstantáneas) a fin de admitir reglas automatizadas para las tareas de administración del ciclo de vida de las imágenes.

`EC2ImageBuilderLifecycleExecutionPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `EC2ImageBuilderLifecycleExecutionPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 16 de noviembre de 2023 a las 23:23 h UTC
- Hora de edición: 16 de noviembre de 2023 a las 23:23 h UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2InstanceConnect

Descripción: Permite a los clientes llamar a EC2 Instance Connect para publicar claves efímeras en sus EC2 instancias y conectarse mediante ssh o la CLI de Instance EC2 Connect.

`EC2InstanceConnect` es una política administrada de AWS.

Uso de la política

Puede asociar `EC2InstanceConnect` a los usuarios, grupos y roles.

Información de la política

- Tipo: política administrada AWS
- Hora de creación: 27 de junio de 2019 a las 18:53 UTC
- Hora de edición: 27 de junio de 2019 a las 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Ec2InstanceConnectEndpoint

Descripción: Política de puntos de conexión de EC2 Instance Connect para gestionar los puntos de conexión de EC2 Instance Connect creados por el cliente

`Ec2InstanceConnectEndpoint` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de enero de 2023 a las 20:19 UTC
- Hora de edición: 24 de enero de 2023 a las 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2InstanceProfileForImageBuilder

Descripción: Perfil de EC2 instancia para el servicio Image Builder.

`EC2InstanceProfileForImageBuilder` es una política administrada de AWS.

Uso de la política

Puede asociar `EC2InstanceProfileForImageBuilder` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de diciembre de 2019 a las 19:08 UTC
- Hora editada: 19 de mayo de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Versión de la política

Versión de la política: v6 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EC2InstanceProfileForImageBuilderECRContainerBuilds

Descripción: Perfil de EC2 instancia para crear imágenes de contenedores con EC2 Image Builder. Esta política otorga al usuario amplios permisos para cargar imágenes de ECR.

`EC2InstanceProfileForImageBuilderECRContainerBuilds` es una política administrada de AWS.

Uso de la política

Puede asociar `EC2InstanceProfileForImageBuilderECRContainerBuilds` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de diciembre de 2020 a las 19:48 UTC
- Hora de edición: 11 de diciembre de 2020 a las 19:48 UTC

- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ECRReplicationServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o administrados por ECR Replication

`ECRReplicationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 4 de diciembre de 2020 a las 22:11 UTC
- Hora de edición: 4 de diciembre de 2020 a las 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ECRTemplateServiceRolePolicy

Descripción: Permite realizar acciones cuando se utilizan plantillas de creación de repositorios de AWS ECR

`ECRTemplateServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 19 de junio de 2024 a las 23:11 h UTC
- Hora de edición: 19 de junio de 2024 a las 23:11 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
```

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElastiCacheServiceRolePolicy

Descripción: Esta política permite ElastiCache administrar AWS los recursos en su nombre según sea necesario para administrar su caché

`ElastiCacheServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de diciembre de 2017 a las 17:50 UTC
- Hora de edición: 28 de noviembre de 2023 a las 03:05 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElasticLoadBalancingFullAccess

Descripción: proporciona acceso completo a Amazon ElasticLoadBalancing y acceso limitado a otros servicios necesarios para proporcionar ElasticLoadBalancing funciones.

`ElasticLoadBalancingFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElasticLoadBalancingFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de septiembre de 2018 a las 20:42 UTC
- Hora de edición: 24 de octubre de 2024 a las 22:21 h UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElasticLoadBalancingReadOnly

Descripción: Proporciona acceso de solo lectura a Amazon ElasticLoadBalancing y a los servicios dependientes

`ElasticLoadBalancingReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `ElasticLoadBalancingReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de septiembre de 2018 a las 20:17 UTC

- Hora de edición: 26 de noviembre de 2023 a las 18:15 h UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalActivationsDownloadSoftwareAccess

Descripción: acceso para ver los activos comprados y descargar el software relacionado y los archivos de inicio

`ElementalActivationsDownloadSoftwareAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalActivationsDownloadSoftwareAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 8 de septiembre de 2020 a las 17:26 UTC
- Hora de edición: 8 de septiembre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalActivationsFullAccess

Descripción: acceso completo para ver y tomar acciones sobre los activos adquiridos en Elemental Appliances y Software

`ElementalActivationsFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalActivationsFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 4 de junio de 2020 a las 21:00 UTC
- Hora de edición: 4 de junio de 2020 a las 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalActivationsGenerateLicenses

Descripción: acceso para ver los activos comprados y generar licencias de software para las activaciones pendientes

`ElementalActivationsGenerateLicenses` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalActivationsGenerateLicenses` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de agosto de 2020 a las 18:28 UTC
- Hora de edición: 28 de agosto de 2020 a las 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalActivationsReadOnlyAccess

Descripción: Acceso de solo lectura a la lista detallada de los activos comprados asociados a los Cuenta de AWS del usuario

`ElementalActivationsReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalActivationsReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 28 de agosto de 2020 a las 16:51 UTC
- Hora de edición: 28 de agosto de 2020 a las 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalAppliancesSoftwareFullAccess

Descripción: acceso completo para ver y tomar acciones sobre las cotizaciones y pedidos de Elemental Appliances y Software

`ElementalAppliancesSoftwareFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalAppliancesSoftwareFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 31 de julio de 2019 a las 16:28 UTC
- Hora de edición: 5 de febrero de 2021 a las 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalAppliancesSoftwareReadOnlyAccess

Descripción: acceso de solo lectura para ver las cotizaciones y los pedidos de Elemental Appliances y Software

`ElementalAppliancesSoftwareReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalAppliancesSoftwareReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 1 de abril de 2020 a las 22:31 UTC
- Hora de edición: 1 de abril de 2020 a las 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ElementalSupportCenterFullAccess

Descripción: acceso completo para ver y tomar acciones en casos de soporte de Elemental Appliance y Software, así como en contenido de soporte de productos

`ElementalSupportCenterFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ElementalSupportCenterFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de noviembre de 2020 a las 18:08 UTC
- Hora de edición: 5 de febrero de 2021 a las 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

EMRDescribeClusterPolicyForEMRWAL

Descripción: esta política concede permisos de solo lectura que permiten al servicio WAL de Amazon EMR encontrar y devolver el estado de un clúster

`EMRDescribeClusterPolicyForEMRWAL` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de junio de 2023 a las 23:30 UTC
- Hora de edición: 15 de junio de 2023 a las 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

FMSServiceRolePolicy

Descripción: Política de acceso que permite a un rol vinculado al servicio de FM realizar acciones relacionadas con FM en los recursos gestionados por FM dentro de la cuenta de la organización de un cliente. AWS

`FMSServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de marzo de 2018 a las 23:01 UTC
- Hora editada: 21 de mayo de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Versión de la política

Versión de la política: v32 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

FSxDeleteServiceLinkedRoleAccess

Descripción: Permite FSx a Amazon eliminar sus funciones vinculadas a servicios para el acceso a Amazon S3

`FSxDeleteServiceLinkedRoleAccess` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 28 de noviembre de 2018 a las 10:40 UTC
- Hora de edición: 28 de noviembre de 2018 a las 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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_*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GameLiftContainerFleetPolicy

Descripción: Otorga los permisos necesarios para procesar acciones en una flota de GameLift contenedores de Amazon, incluido el acceso a dependencias como Amazon S3.

`GameLiftContainerFleetPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `GameLiftContainerFleetPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 12 de noviembre de 2024 a las 19:28 UTC
- Hora editada: 5 de febrero de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GameLiftGameServerGroupPolicy

Descripción: Política que permite a Gamelift gestionar los recursos GameServerGroups de los clientes

`GameLiftGameServerGroupPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `GameLiftGameServerGroupPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 3 de abril de 2020 a las 23:12 UTC
- Hora de edición: 13 de mayo de 2020 a las 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GitLabDuoWithAmazonQPermissionsPolicy

Descripción: Esta política gestionada concede permiso para conectarse con Amazon Q y utilizar las funciones de la integración GitLab Duo con Amazon Q.

`GitLabDuoWithAmazonQPermissionsPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `GitLabDuoWithAmazonQPermissionsPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 16 de abril de 2025 a las 16:37 UTC
- Hora editada: 16 de abril de 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GlobalAcceleratorFullAccess

Descripción: Permitir a GlobalAccelerator los usuarios el acceso completo a todos APIs

`GlobalAcceleratorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `GlobalAcceleratorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 02:44 UTC
- Hora de edición: 4 de diciembre de 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GlobalAcceleratorReadOnlyAccess

Descripción: Permitir a GlobalAccelerator los usuarios el acceso de solo lectura APIs

`GlobalAcceleratorReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `GlobalAcceleratorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 02:41 UTC
- Hora de edición: 27 de noviembre de 2018 a las 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GreengrassOTAUpdateArtifactAccess

Descripción: proporciona acceso de lectura a los artefactos de actualización OTA de Greengrass en todas las regiones de Greengrass

`GreengrassOTAUpdateArtifactAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `GreengrassOTAUpdateArtifactAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio

- Hora de creación: 29 de noviembre de 2017 a las 18:11 UTC
- Hora de edición: 18 de diciembre de 2018 a las 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GroundTruthSyntheticConsoleFullAccess

Descripción: Esta política otorga los permisos necesarios para usar todas las funciones de la consola sintética SageMaker Ground Truth.

`GroundTruthSyntheticConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `GroundTruthSyntheticConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 25 de agosto de 2022 a las 15:58 UTC
- Hora de edición: 25 de agosto de 2022 a las 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
```

```
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

GroundTruthSyntheticConsoleReadOnlyAccess

Descripción: Esta política otorga acceso de solo lectura a SageMaker Ground Truth Synthetic a través del. AWS Management Console

`GroundTruthSyntheticConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `GroundTruthSyntheticConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 25 de agosto de 2022 a las 15:58 UTC
- Hora de edición: 25 de agosto de 2022 a las 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Health_OrganizationsServiceRolePolicy

Descripción: Política AWS de salud para habilitar la función de vista organizacional

`Health_OrganizationsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de diciembre de 2019 a las 13:28 UTC
- Hora de edición: 06 de febrero de 2024 a las 16:07 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMAccessAdvisorReadOnly

Descripción: esta política concede acceso para leer toda la información de acceso que el asesor de acceso de IAM proporciona, como la información del último servicio al que se accedió.

`IAMAccessAdvisorReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMAccessAdvisorReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 21 de junio de 2019 a las 19:33 UTC
- Hora de edición: 21 de junio de 2019 a las 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMAccessAnalyzerFullAccess

Descripción: proporciona acceso completo al Analizador de acceso de IAM

`IAMAccessAnalyzerFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMAccessAnalyzerFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de diciembre de 2019 a las 17:12 UTC
- Hora de edición: 2 de diciembre de 2019 a las 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMAccessAnalyzerReadOnlyAccess

Descripción: proporciona acceso de solo lectura a los recursos del Analizador de acceso de IAM

`IAMAccessAnalyzerReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMAccessAnalyzerReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 2 de diciembre de 2019 a las 17:12 UTC
- Hora de edición: 18 de julio de 2024 a las 17:49 h UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
```

```
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMFullAccess

Descripción: Proporciona acceso completo a IAM a través del AWS Management Console.

`IAMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 21 de junio de 2019 a las 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a IAM a través del AWS Management Console.

`IAMReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:40 UTC
- Hora de edición: 25 de enero de 2018 a las 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMSelfManageServiceSpecificCredentials

Descripción: permite a un usuario de IAM administrar sus propias credenciales específicas del servicio.

`IAMSelfManageServiceSpecificCredentials` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMSelfManageServiceSpecificCredentials` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de diciembre de 2016 a las 17:25 UTC
- Hora de edición: 22 de diciembre de 2016 a las 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMUserChangePassword

Descripción: proporciona a un usuario de IAM la posibilidad de cambiar su propia contraseña.

`IAMUserChangePassword` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMUserChangePassword` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 15 de noviembre de 2016 a las 00:25 UTC
- Hora editada: 29 de mayo de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Versión de la política

Versión de la política: v3 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IAMUserSSHKeys

Descripción: proporciona a un usuario de IAM la posibilidad de administrar sus propias claves SSH.

`IAMUserSSHKeys` es una política administrada de AWS.

Uso de la política

Puede asociar `IAMUserSSHKeys` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de julio de 2015 a las 17:08 UTC
- Hora de edición: 9 de julio de 2015 a las 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IVSFullAccess

Descripción: proporciona acceso completo al Servicio de video interactivo (IVS). También incluye permisos para los servicios dependientes, necesarios para el acceso completo a la consola de IVS.

`IVSFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IVSFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada

- Hora de creación: 13 de diciembre de 2023 a las 21:20 h UTC
- Hora de edición: 13 de diciembre de 2023 a las 21:20 h UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IVSReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la transmisión de IVS de baja latencia y en tiempo real APIs

`IVSReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `IVSReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 05 de diciembre de 2023 a las 18:00 h UTC
- Hora de edición: 17 de septiembre de 2024 a las 20:42 h UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

IVSRecordToS3

Descripción: Función vinculada al servicio que permite desde S3 PutObject hasta la grabación de transmisiones en directo del IVS

`IVSRecordToS3` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de diciembre de 2020 a las 00:10 UTC
- Hora de edición: 5 de diciembre de 2020 a las 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

KafkaConnectServiceRolePolicy

Descripción: Esta política concede a Kafka Connect permiso para gestionar AWS los recursos en su nombre.

`KafkaConnectServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de septiembre de 2021 a las 13:12 UTC
- Hora de edición: 7 de septiembre de 2021 a las 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

KafkaServiceRolePolicy

Descripción: política de rol vinculado al servicio para Kafka.

`KafkaServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de noviembre de 2018 a las 23:31 UTC
- Hora de edición: 28 de abril de 2023 a las 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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_*"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

KeyspacesCDCServiceRolePolicy

Descripción: Otorga los permisos necesarios a Amazon Keyspaces for Change Data Capture

`KeyspacesCDCServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 21 de junio de 2025 a las 00:22 UTC
- Hora editada: 21 de junio de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

KeyspacesReplicationServiceRolePolicy

Descripción: permisos requeridos por Keyspaces para la replicación de datos entre regiones

`KeyspacesReplicationServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2023 a las 16:15 UTC
- Hora editada: 15 de noviembre de 2024 a las 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

LakeFormationDataAccessServiceRolePolicy

Descripción: política para conceder acceso temporal a los datos de los recursos de Lake Formation

`LakeFormationDataAccessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 20 de junio de 2019 a las 20:46 UTC

- Hora de edición: 06 de febrero de 2024 a las 18:37 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

LexBotPolicy

Descripción: Política para el caso de uso de AWS Lex Bot

`LexBotPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2017 a las 22:18 UTC
- Hora de edición: 13 de noviembre de 2019 a las 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

LexChannelPolicy

Descripción: Política para el caso de uso de AWS Lex Channel

`LexChannelPolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de febrero de 2017 a las 23:23 UTC
- Hora de edición: 17 de febrero de 2017 a las 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

LightsailExportAccess

Descripción: Política de roles vinculados AWS al servicio Lightsail que otorga permisos para exportar recursos

`LightsailExportAccess` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio

- Hora de creación: 28 de septiembre de 2018 a las 16:35 UTC
- Hora de edición: 15 de enero de 2022 a las 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MediaConnectGatewayInstanceRolePolicy

Descripción: Esta política otorga permiso para registrar instancias de MediaConnect puerta de enlace en una MediaConnect puerta de enlace.

`MediaConnectGatewayInstanceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `MediaConnectGatewayInstanceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 22 de marzo de 2023 a las 20:43 UTC
- Hora de edición: 22 de marzo de 2023 a las 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MediaPackageServiceRolePolicy

Descripción: Permite MediaPackage publicar registros en CloudWatch

`MediaPackageServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de septiembre de 2020 a las 17:45 UTC
- Hora de edición: 18 de septiembre de 2020 a las 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MemoryDBServiceRolePolicy

Descripción: Esta política permite a MemoryDB administrar AWS los recursos en su nombre según sea necesario para administrar sus recursos.

`MemoryDBServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 17 de agosto de 2021 a las 22:34 UTC
- Hora editada: 1 de diciembre de 2024 a las 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
    }
  ]
```

```
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MigrationHubDMSAccessServiceRolePolicy

Descripción: política para que Database Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

`MigrationHubDMSAccessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2019 a las 17:50 UTC
- Hora de edición: 7 de octubre de 2019 a las 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MigrationHubServiceRolePolicy

Descripción: permite que Migration Hub llame a Application Discovery Service en su nombre

`MigrationHubServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2019 a las 17:22 UTC
- Hora de edición: 6 de agosto de 2020 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MigrationHubSMSAccessServiceRolePolicy

Descripción: política para que Server Migration Service asuma un rol en la cuenta del cliente para llamar a Migration Hub

`MigrationHubSMSAccessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de junio de 2019 a las 18:30 UTC
- Hora de edición: 7 de octubre de 2019 a las 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MonitronServiceRolePolicy

Descripción: Política para el rol vinculado al servicio de AWS Monitron que otorga acceso a los recursos de los clientes requeridos.

`MonitronServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 2 de mayo de 2022 a las 19:22 UTC
- Hora de edición: 2 de mayo de 2022 a las 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MultiPartyApprovalFullAccess

Descripción: Proporciona acceso completo a la aprobación multipartita. Esta política también incluye los permisos relacionados con AWS Organizations e AWS IAM Identity para gestionar los equipos de aprobación y las fuentes de identidad.

`MultiPartyApprovalFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `MultiPartyApprovalFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2025 a las 20:22 UTC
- Hora editada: 18 de junio de 2025 a las 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

MultiPartyApprovalReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la aprobación multipartita. Esta política también incluye permisos de lectura relacionados con AWS Organizations e AWS IAM Identity para los equipos de aprobación y las fuentes de identidad.

`MultiPartyApprovalReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `MultiPartyApprovalReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 18 de junio de 2025 a las 20:07 UTC
- Hora editada: 18 de junio de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NeptuneConsoleFullAccess

Descripción: proporciona acceso completo para administrar Amazon Neptune mediante la AWS Management Console. Tenga en cuenta que esta política también otorga acceso total para publicar sobre todos los temas de SNS de la cuenta, permisos para crear y editar EC2 instancias de

Amazon y configuraciones de VPC, permisos para ver y enumerar claves en Amazon KMS y acceso completo a Amazon RDS. Para obtener más información, consulte las preguntas frecuentes/. https://aws.amazon.com/neptune/

`NeptuneConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `NeptuneConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 19 de junio de 2018 a las 21:35 UTC
- Hora de edición: 30 de noviembre de 2023 a las 07:32 h UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
```

```
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NeptuneFullAccess

Descripción: proporciona acceso completo a Amazon Neptune. Tenga en cuenta que esta política también otorga acceso total a las publicaciones sobre todos los temas de SNS de la cuenta, y brinda acceso total a Amazon RDS. Para obtener más información, consulte las preguntas https://aws.amazon.com/neptune/ frecuentes/.

`NeptuneFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `NeptuneFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de mayo de 2018 a las 19:17 UTC
- Hora de edición: 22 de enero de 2024 a las 16:32 h UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NeptuneGraphReadOnlyAccess

Descripción: proporciona acceso de solo lectura a todos los recursos de análisis por Amazon Neptune junto con permisos de solo lectura para servicios dependientes.

`NeptuneGraphReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `NeptuneGraphReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de noviembre de 2023 a las 07:32 h UTC
- Hora de edición: 30 de noviembre de 2023 a las 07:32 h UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NeptuneReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Amazon Neptune. Tenga en cuenta que esta política también concede acceso a los recursos de Amazon RDS. Para obtener más información, consulte las preguntas https://aws.amazon.com/neptune/ frecuentes/.

`NeptuneReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `NeptuneReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de mayo de 2018 a las 19:16 UTC
- Hora de edición: 22 de enero de 2024 a las 16:33 h UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NetworkAdministrator

Descripción: Otorga permisos de acceso total a AWS los servicios y acciones necesarios para configurar y configurar los recursos AWS de la red.

`NetworkAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `NetworkAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:31 UTC
- Hora editada: 19 de diciembre de 2024 a las 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Versión de la política

Versión de la política: v13 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:*",
        "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

NetworkSecurityDirectorServiceLinkedRolePolicy

Descripción: Proporciona permisos para que el rol vinculado al servicio de director de seguridad de red AWS Shield evalúe entornos específicos.

`NetworkSecurityDirectorServiceLinkedRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 13 de junio de 2025 a las 20:07 UTC
- Hora editada: 13 de junio de 2025 a las 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

OAMFullAccess

Descripción: Proporciona acceso completo a CloudWatch Observability Access Manager

`OAMFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `OAMFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 13:38 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

OAMReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a CloudWatch Observability Access Manager

`OAMReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `OAMReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2022 a las 13:29 UTC
- Hora de edición: 27 de noviembre de 2022 a las 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

OpensearchIngestionSelfManagedVpcePolicy

Descripción: Permite a Amazon OpenSearch Ingestion describir los recursos de la red y escribir métricas de servicio en Cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 10 de junio de 2024 a las 19:59 h UTC
- Hora de edición: 10 de junio de 2024 a las 19:59 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

PartnerCentralAccountManagementUserRoleAssociation

Descripción: proporciona acceso para asociar los usuarios centrales de los socios a roles de IAM y desasociarlos de estos

`PartnerCentralAccountManagementUserRoleAssociation` es una política administrada de AWS.

Uso de la política

Puede asociar `PartnerCentralAccountManagementUserRoleAssociation` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 10 de noviembre de 2023 a las 02:03 UTC
- Hora de edición: 10 de noviembre de 2023 a las 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

PowerUserAccess

Descripción: Proporciona acceso completo a AWS los servicios y recursos, pero no permite la administración de usuarios y grupos.

`PowerUserAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `PowerUserAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 29 de abril de 2025 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

QAppsServiceRolePolicy

Descripción: Otorga permisos Servicios de AWS y recursos utilizados o gestionados por Amazon Q Apps.

`QAppsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 26 de septiembre de 2024 a las 19:22 h UTC
- Hora de edición: 26 de septiembre de 2024 a las 19:22 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

QBusinessQuicksightPluginPolicy

Descripción: Otorga permisos QBusiness QuickSight APIs para solicitar el QuickSight complemento

`QBusinessQuicksightPluginPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `QBusinessQuicksightPluginPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 3 de diciembre de 2024 a las 15:36 UTC
- Hora editada: 3 de diciembre de 2024 a las 15:36 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

QBusinessServiceRolePolicy

Descripción: Otorga permisos Servicios de AWS y recursos utilizados o gestionados por Amazon Q

`QBusinessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de abril de 2024 a las 16:05 h UTC
- Hora de edición: 29 de abril de 2024 a las 16:05 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Descripción: Política utilizada por el QuickSight equipo para acceder a los datos de los clientes generados por S3 Storage Management Analytics.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 12 de junio de 2017 a las 18:18 UTC
- Hora de edición: 8 de octubre de 2019 a las 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

RDSCloudHsmAuthorizationRole

Descripción: política predeterminada para el rol de servicio de Amazon RDS.

`RDSCloudHsmAuthorizationRole` es una política administrada de AWS.

Uso de la política

Puede asociar `RDSCloudHsmAuthorizationRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 26 de septiembre de 2019 a las 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a los AWS servicios y recursos.

`ReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora editada: 3 de junio de 2025 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Versión de la política

Versión de la política: v129 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
```

```
        "aiops:ListInvestigations",
        "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:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
```

```
        "appconfig:ListDeployments",
        "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:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "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:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestRuns",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
```

```
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "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",
        "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: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:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListAgents",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "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:ListCustomLineItemVersions",
        "billingconductor:ListCustomLineItems",
```

```
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "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:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "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: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: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:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "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:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
```

```
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "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:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListPackages",
        "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*",
        "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:ListTargets",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "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:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListRecommendations",
        "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:ListRecipeVersions",
        "databrew:ListRecipes",
        "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:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "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:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "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:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
```

```
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "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: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*",
        "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:ListClusters",
        "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:DescribeImageTags",
        "ecr-public:DescribeImages",
        "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:List*",
        "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*",
        "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:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "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:GetDetectorVersion",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetModels",
```

```
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "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:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
```

```
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetMapping",
        "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:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "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:ListSchemaVersions",
        "glue:ListSchemas",
        "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:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "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*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
```

```
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectorModels",
        "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:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "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:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "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:ListStageSessions",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreamSessions",
        "ivs:ListStreams",
        "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:ListDataSourceSyncJobs",
        "kendra:ListDataSources",
        "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:ListBotAliasReplicas",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "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:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "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:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
```

```
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "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:ListModelVersions",
        "lookoutequipment:ListModels",
        "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:ListApplicationVersions",
        "m2:ListApplications",
        "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:GetFindingStatistics",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "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:ListProposalVotes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
```

```
        "mediaconvert:List*",
        "medialive:DescribeChannel",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "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:ListInputDeviceTransfers",
        "medialive:ListInputDevices",
        "medialive:ListInputSecurityGroups",
        "medialive:ListInputs",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "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:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "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",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
```

```
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetConnections",
        "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:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager: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:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "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:ListEnvironmentTemplates",
        "proton:ListEnvironments",
        "proton:ListServiceInstances",
        "proton:ListServiceTemplates",
        "proton:ListServices",
        "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:ListDataSourceSyncJobs",
        "qbusiness:ListDataSources",
        "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:ListEnvironmentVpcs",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeProjects",
```

```
        "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: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:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
```

```
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "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*",
        "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*",
        "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*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
```

```
        "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*",
        "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:GetAWSDefaultServiceQuota",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "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:DescribeOptOutLists",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribePhoneNumbers",
```

```
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "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:GetDatabase",
        "ssm-sap:GetOperation",
        "ssm-sap:GetResourcePermission",
        "ssm-sap:ListApplications",
        "ssm-sap:ListComponents",
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "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:DescribeSupportLevel",
        "support:DescribeSupportedLanguages",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorChecks",
        "support:SearchForCases",
```

```
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "sustainability:GetCarbonFootprintSummary",
        "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",
        "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",
        "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: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: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:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ResourceGroupsandTagEditorFullAccess

Descripción: proporciona acceso completo a los Grupos de recursos y el Editor de etiquetas.

`ResourceGroupsandTagEditorFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ResourceGroupsandTagEditorFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 10 de agosto de 2023 a las 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Versión de la política

Versión de la política: v6 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ResourceGroupsandTagEditorReadOnlyAccess

Descripción: proporciona acceso para utilizar los Grupos de recursos y el Editor de etiquetas, pero no permite editar etiquetas con el Editor de etiquetas.

`ResourceGroupsandTagEditorReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ResourceGroupsandTagEditorReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:39 UTC
- Hora de edición: 10 de agosto de 2023 a las 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ResourceGroupsServiceRolePolicy

Descripción: Permite a AWS Resource Groups consultar los AWS servicios que son propietarios de sus recursos para conservar el grupo up-to-date

`ResourceGroupsServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 5 de enero de 2023 a las 16:57 UTC
- Hora de edición: 5 de enero de 2023 a las 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ResourceGroupsTaggingAPITagUntagSupportedResources

Descripción: proporciona permisos para etiquetar y quitar etiquetas de todos los recursos compatibles con la API de etiquetado de los Grupos de recursos. Esta política también concede los permisos necesarios para recuperar todos los recursos etiquetados o previamente etiquetados a través de la API de etiquetado de los Grupos de recursos.

`ResourceGroupsTaggingAPITagUntagSupportedResources` es una política administrada de AWS.

Uso de la política

Puede asociar `ResourceGroupsTaggingAPITagUntagSupportedResources` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de octubre de 2024 a las 11:11 h UTC
- Hora editada: 11 de diciembre de 2024 a las 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAAmazonEBSCSIDriverOperatorPolicy

Descripción: Permite que el operador del controlador de la interfaz de almacenamiento de contenedores (CSI) de OpenShift Amazon EBS instale y mantenga el controlador CSI de Amazon EBS en un clúster de Red Hat OpenShift Service on AWS (ROSA). El controlador de CSI de Amazon EBS permite que los clústeres de ROSA administren el ciclo de vida de los volúmenes de Amazon EBS para volúmenes persistentes.

`ROSAAmazonEBSCSIDriverOperatorPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAAmazonEBSCSIDriverOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:36 UTC
- Hora de edición: 22 de enero de 2025 a las 00:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSACloudNetworkConfigOperatorPolicy

Descripción: Permite al operador del OpenShift Cloud Network Config Controller aprovisionar y gestionar los recursos de red para que los utilice el OpenShift Servicio Red Hat en la superposición de redes de clústeres AWS (ROSA). El operador de red OpenShift en la nube interactúa con los complementos de red AWS APIs en nombre de los complementos de red mediante CustomResourceDefinitions. El operador utiliza estos permisos de política para gestionar las direcciones IP privadas de las EC2 instancias de Amazon como parte del clúster ROSA.

`ROSACloudNetworkConfigOperatorPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSACloudNetworkConfigOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:34 UTC
- Hora de edición: 20 de abril de 2023 a las 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAControlPlaneOperatorPolicy

Descripción: Permite a Red Hat OpenShift Service on AWS (ROSA) gestionar los recursos de Amazon EC2 y Amazon Route 53 del clúster ROSA.

`ROSAControlPlaneOperatorPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAControlPlaneOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 24 de abril de 2023 a las 23:02 UTC
- Hora editada: 10 de abril de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "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/*"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAImageRegistryOperatorPolicy

Descripción: Permite al operador de registro de OpenShift imágenes aprovisionar y administrar buckets y objetos de Amazon S3 para que los utilice el OpenShift Servicio Red Hat en el registro de imágenes integrado en el clúster AWS (ROSA) a fin de cumplir con los requisitos de almacenamiento

de ROSA. El operador OpenShift de registro de imágenes instala y mantiene el registro interno de un clúster de Red Hat. OpenShift

`ROSAImageRegistryOperatorPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAImageRegistryOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:13 UTC
- Hora editada: 19 de mayo de 2025 a las 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM

- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAIngressOperatorPolicy

Descripción: Permite al operador de OpenShift ingreso aprovisionar y administrar los balanceadores de carga y las configuraciones del sistema de nombres de dominio (DNS) para los clústeres de Red Hat OpenShift Service on AWS (ROSA). La política concede acceso de lectura a los valores de las etiquetas, que el operador filtra para que los recursos de Route 53 descubran las zonas alojadas.

`ROSAIngressOperatorPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAIngressOperatorPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:37 UTC
- Hora editada: 10 de abril de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAInstallerPolicy

Descripción: Permite que el instalador de Red Hat OpenShift Service on AWS (ROSA) administre AWS los recursos que respaldan la instalación del clúster ROSA. Esto incluye la gestión de los perfiles de instancia para los nodos de trabajo de ROSA.

`ROSAInstallerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAInstallerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 6 de junio de 2023 a las 21:00 UTC
- Hora de edición: 10 de abril de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "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" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAKMSProviderPolicy

Descripción: Permite que el proveedor de AWS cifrado ROSA integrado administre las AWS claves del Servicio de administración de claves (KMS) para respaldar el cifrado de datos etcd utilizando una clave AWS KMS proporcionada por el cliente. La política permite cifrar y descifrar los datos con las claves KMS.

`ROSAKMSProviderPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAKMSProviderPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:10 UTC
- Hora de edición: 27 de abril de 2023 a las 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAKubeControllerPolicy

Descripción: Permite que el controlador de Kubernetes ROSA administre los recursos de Amazon EC2, Elastic Load Balancing (ELB) y AWS Key Management Service (KMS) para un clúster ROSA.

`ROSAKubeControllerPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAKubeControllerPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de abril de 2023 a las 20:09 UTC
- Hora de edición: 10 de abril de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAManageSubscription

Descripción: Esta política proporciona los permisos necesarios para administrar la suscripción a Red Hat OpenShift Service on AWS (ROSA).

`ROSAManageSubscription` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAManageSubscription` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 11 de abril de 2022 a las 20:58 UTC

- Hora de edición: 4 de agosto de 2023 a las 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSANodePoolManagementPolicy

Descripción: Permite a Red Hat OpenShift Service on AWS (ROSA) administrar las EC2 instancias del clúster como nodos de trabajo, incluido el permiso para configurar grupos de seguridad y etiquetar instancias y volúmenes. Esta política también permite el uso de EC2 instancias con cifrado de disco proporcionado por las AWS claves del Servicio de administración de claves (KMS).

`ROSANodePoolManagementPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSANodePoolManagementPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 8 de junio de 2023 a las 20:48 UTC
- Hora editada: 5 de mayo de 2025 a las 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "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/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
```

```
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSASRESupportPolicy

Descripción: proporciona al departamento de ingeniería de confiabilidad de sitios (SRE) de ROSA los permisos necesarios para observar, diagnosticar y respaldar inicialmente AWS los recursos asociados con el OpenShift Servicio Red Hat en los clústeres AWS (ROSA), incluida la capacidad de cambiar el estado de los nodos del clúster ROSA.

`ROSASRESupportPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSASRESupportPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 1 de junio de 2023 a las 14:36 UTC
- Hora de edición: 10 de abril de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ROSAWorkerInstancePolicy

Descripción: Permite que Red Hat OpenShift Service on AWS (ROSA) de los nodos de trabajo de su cuenta tenga acceso de solo lectura a las EC2 instancias de Amazon y a la administración del ciclo de vida de Regiones de AWS los nodos de cómputo.

`ROSAWorkerInstancePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `ROSAWorkerInstancePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de abril de 2023 a las 22:35 UTC
- Hora de edición: 20 de marzo de 2025 a las 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Route53RecoveryReadinessServiceRolePolicy

Descripción: política de rol vinculado al servicio para la Preparación para la recuperación de Route 53.

`Route53RecoveryReadinessServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 15 de julio de 2021 a las 16:06 UTC
- Hora de edición: 14 de febrero de 2023 a las 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Route53ResolverServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o administrados por Route53 Resolver

`Route53ResolverServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 12 de agosto de 2020 a las 17:47 UTC
- Hora de edición: 12 de agosto de 2020 a las 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

S3StorageLensServiceRolePolicy

Descripción: Permite el acceso a Servicios de AWS los recursos utilizados o gestionados por S3 Storage Lens

`S3StorageLensServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 18 de noviembre de 2020 a las 18:15 UTC
- Hora de edición: 18 de noviembre de 2020 a las 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioAdminProjectUserRolePolicy

Descripción: Esta política de IAM otorga a un rol de IAM acceso total al catálogo de datos de AWS Glue (metadatos) y a Amazon S3 (datos reales) para las operaciones de lagos de datos, con el acceso limitado por cuenta y etiquetas de rol.

`SageMakerStudioAdminProjectUserRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioAdminProjectUserRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 9 de julio de 2025 a las 20:52 UTC
- Hora editada: 9 de julio de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockAgentServiceRolePolicy

Descripción: Permite a los agentes de Amazon Bedrock acceder a los modelos de Amazon Bedrock y a otros recursos adjuntos a un agente en SageMaker Studio.

`SageMakerStudioBedrockAgentServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockAgentServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 13 de febrero de 2025 a las 23:37 UTC
- Hora editada: 13 de febrero de 2025 a las 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockChatAgentUserRolePolicy

Descripción: Proporciona acceso a la configuración de una aplicación de agente de chat de Amazon Bedrock y al agente de Amazon Bedrock en SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockChatAgentUserRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 13 de febrero de 2025 a las 23:52 UTC
- Hora editada: 13 de febrero de 2025 a las 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Descripción: Permite a Amazon Bedrock acceder a los modelos y conjuntos de datos de Amazon Bedrock para trabajos de evaluación en Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de febrero de 2025 a las 00:37 UTC
- Hora editada: 14 de febrero de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockFlowServiceRolePolicy

Descripción: Permite a Amazon Bedrock Flows acceder a los modelos de Amazon Bedrock y a otros recursos adjuntos a un flujo en SageMaker Studio.

`SageMakerStudioBedrockFlowServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockFlowServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de febrero de 2025 a las 00:07 UTC
- Hora editada: 9 de abril de 2025 a las 20:37 UTC

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

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockFunctionExecutionRolePolicy

Descripción: Permite a AWS Lambda acceder a la configuración de un componente de función de Amazon Bedrock en Studio. SageMaker

`SageMakerStudioBedrockFunctionExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockFunctionExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de febrero de 2025 a las 03:52 UTC
- Hora editada: 25 de febrero de 2025 a las 03:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Descripción: Proporciona acceso para configurar los almacenes vectoriales y las bases de conocimiento de Amazon Bedrock en SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de febrero de 2025 a las 03:37 UTC
- Hora editada: 25 de febrero de 2025 a las 03:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Descripción: Permite a Amazon Bedrock Knowledge Bases acceder a los modelos y fuentes de datos de Amazon Bedrock en SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 25 de febrero de 2025 a las 02:52 UTC
- Hora editada: 16 de abril de 2025 a las 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioBedrockPromptUserRolePolicy

Descripción: Proporciona acceso a un indicador de Amazon Bedrock y a su configuración en SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioBedrockPromptUserRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 14 de febrero de 2025 a las 00:22 UTC
- Hora editada: 14 de febrero de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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}/*"
          ]
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioDomainExecutionRolePolicy

Descripción: Amazon SageMaker Studio utiliza esta política para catalogar, descubrir, gobernar, compartir y analizar los datos del dominio de Amazon SageMaker Studio.

`SageMakerStudioDomainExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioDomainExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de noviembre de 2024 a las 21:56 UTC
- Hora editada: 17 de junio de 2025 a las 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "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:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetConnection",
        "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:GetUpdateEligibility",
```

```
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "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: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/*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioDomainServiceRolePolicy

Descripción: Función de servicio para las acciones a nivel de dominio en el portal que realiza Amazon SageMaker Studio.

`SageMakerStudioDomainServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioDomainServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de noviembre de 2024 a las 21:56 UTC
- Hora editada: 20 de noviembre de 2024 a las 21:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioEMRInstanceRolePolicy

Descripción: Amazon SageMaker Studio crea funciones de IAM para que los usuarios de los proyectos realicen acciones de análisis de datos, inteligencia artificial y aprendizaje automático, y utiliza esta política al crear estas funciones para definir los permisos relacionados con el EMR.

`SageMakerStudioEMRInstanceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioEMRInstanceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 27 de febrero de 2025 a las 00:22 UTC
- Hora editada: 27 de febrero de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${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}"
        }
      }
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioEMRServiceRolePolicy

Descripción: Amazon SageMaker Studio crea funciones de IAM para que los usuarios de los proyectos realicen acciones de análisis de datos, inteligencia artificial y aprendizaje automático, y utiliza esta política al crear estas funciones para definir los permisos relacionados con el EMR.

`SageMakerStudioEMRServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioEMRServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 31 de enero de 2025 a las 19:52 UTC
- Hora editada: 27 de febrero de 2025 a las 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${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" : "AllowEMRForKMSManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEMRToListKmsAliases",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioFullAccess

Descripción: Esta política proporciona acceso total a Amazon SageMaker Unified Studio a través de la consola SageMaker de administración de Amazon.

`SageMakerStudioFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 28 de noviembre de 2024 a las 00:06 UTC
- Hora editada: 6 de junio de 2025 a las 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Versión de la política

Versión de la política: v4 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "quicksight:DescribeAccountSubscription"
      ],
      "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/*",
        "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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioProjectProvisioningRolePolicy

Descripción: Amazon SageMaker Studio utiliza esta política para aprovisionar y gestionar los recursos de su cuenta.

`SageMakerStudioProjectProvisioningRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioProjectProvisioningRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de noviembre de 2024 a las 21:58 UTC
- Hora editada: 3 de julio de 2025 a las 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Versión de la política

Versión de la política: v16 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codecommit:DeleteRepository",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcList",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMManage",
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamDzManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "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/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
```

```
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamManageAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamManageBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "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"
          ]
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
```

```
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
```

```
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        }
      }
    },
    {
      "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_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        }
      }
    },
    {
      "Sid" : "ManageRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzManageRoles",
      "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" : "DzManagePolicy",
      "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" : "ListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "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_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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"
          ]
        }
      }
    },
    {
      "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${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:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "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" : "GlueConnManage",
      "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}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "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" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageCatalogConn",
      "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"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "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/Serverless*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaUpdate",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "glue.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "s3:prefix" : "true"
        }
      }
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Effect" : "Allow"
    },
    {
      "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" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
```

```
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLG",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageLG",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:DeleteLogGroup",
        "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaManage",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "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"
      ]
    },
    {
      "Sid" : "RedshiftList",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:GetResourcePolicy"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RssDbRole",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift:GetResourcePolicy",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:UpdateNamespace",
```

```
        "redshift-serverless:UpdateWorkgroup",
        "redshift-serverless:UntagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        }
      }
    },
    {
      "Sid" : "GetRandom",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetRandomPassword",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SMDManage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListDomains",
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "EmrSManage",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:DeleteApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "EmrSGetStop",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${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" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "ManageAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetBedrockCfnResourceDefinitionS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "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" : "BRManage",
      "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" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
```

```
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ListBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "ManageBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRManage",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "EMRClusterManage",
      "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" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "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" : "AirflowGet",
      "Effect" : "Allow",
      "Action" : [
```

```
        "airflow:GetEnvironment"
      ],
      "Resource" : "*"
    },
    {
      "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" : "AirflowKmsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleManage",
      "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",
      "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" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : "scheduler:DeleteScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
```

```
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "ManageQSFolder",
      "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" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "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:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
```

```
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioProjectRoleMachineLearningPolicy

Descripción: Amazon SageMaker Studio crea funciones de IAM para que los usuarios de los proyectos realicen acciones de análisis de datos, inteligencia artificial y aprendizaje automático, y utiliza esta política al crear estas funciones para definir los permisos relacionados SageMaker con.

`SageMakerStudioProjectRoleMachineLearningPolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioProjectRoleMachineLearningPolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2024 a las 21:55 UTC
- Hora editada: 14 de abril de 2025 a las 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "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: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"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "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:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
```

```
    {
      "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:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "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:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "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:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "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:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts"
      ],
      "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:ListAssociations",
        "sagemaker:ListHubContents",
```

```
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${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" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "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" : "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "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" : "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" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "application-autoscaling:service-namespace" : "sagemaker"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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" : {
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioProjectUserRolePermissionsBoundary

Descripción: Amazon SageMaker crea funciones de IAM para que los usuarios de Projects realicen acciones de análisis de datos, inteligencia artificial y aprendizaje automático, y utiliza esta política al crear estas funciones para definir el límite de sus permisos.

`SageMakerStudioProjectUserRolePermissionsBoundary` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioProjectUserRolePermissionsBoundary` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2024 a las 21:57 UTC

- Hora editada: 3 de enero de 2025 a las 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioProjectUserRolePolicy

Descripción: Amazon SageMaker Studio crea funciones de IAM para que los usuarios de los proyectos realicen acciones de análisis de datos, inteligencia artificial y aprendizaje automático, y utiliza esta política al crear estas funciones para definir los permisos.

`SageMakerStudioProjectUserRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioProjectUserRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 20 de noviembre de 2024 a las 21:59 UTC
- Hora editada: 25 de junio de 2025 a las 04:22 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Versión de la política

Versión de la política: v14 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CommonUserCodeCommitPermissions",
      "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" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "AllowCodeWhispererGenerateRecommendations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManageGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAttachGlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "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" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "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:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:GetSession",
        "glue:ListStatements",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:GetStatement",
        "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" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueVisualETLPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "arn:aws:glue:*:*:completion/*"
    },
    {
      "Sid" : "GlueJobRunnerSessionLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsPermissionsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "StringEquals" : {
```

```
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessInteractivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "EmrServerlessJobAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun"
      ],
      "Resource" : [
        "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*"
      ],
      "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}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "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" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DataLakeCrossAccountDecryptKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${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" : "AccessDomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectLogGroupPermissions",
      "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" : "DefaultAthenaDataCatalogPermissions",
      "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"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
      "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",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:UseGlueStudio"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "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: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" : "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" : "GlueDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissionForDataLakeAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
```

```
      ],
      "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" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        }
      }
    },
    {
      "Sid" : "SetContextForTrustedIdentityPropagation",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "UnRestrictedAccessForGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
```

```
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "scheduler.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchActionsWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "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",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
    {
      "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" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForResources",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "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"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessWorkgroupWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "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" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "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"
      ],
      "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" : "EMRGetClusterSessionCredentials",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
```

```
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "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" : {
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
```

```
            "redshift.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagementPermissions",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBedrockModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        },
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "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" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        },
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModelAppInferenceProfilePermissions",
      "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" : "BedrockInvokeModelAppInferenceProfilePermissions",
      "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" : "CreateEvaluationJobForFoundationModelPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BedrockCreateEvaluationJobPermissions",
      "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" : "BedrockRetrieveAndGeneratePermissions",
      "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" : "IamPassRoleToBedrockPermissions",
      "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" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForAmazonBedrockIDE",
      "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" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessSecretKmsPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        }
      }
    },
    {
      "Sid" : "KmsViaSecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GetDataZoneEnvironmentCloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudFormationGetDataZoneEnvironmentStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "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" : "FederatedConnectionGetSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionLambdaLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
```

```
    },
    {
      "Sid" : "FederatedConnectionDDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConnectionEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDeleteENIPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDescribeENIPermissions",
      "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" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:UpdateDataCellsFilter",
```

```
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "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" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "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" : "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" : "ManageQuickSightFolderAndDataSourceResources",
      "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" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SageMakerStudioQueryExecutionRolePolicy

Descripción: Amazon SageMaker Studio utiliza esta política al ejecutar consultas en conexiones federadas.

`SageMakerStudioQueryExecutionRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `SageMakerStudioQueryExecutionRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 31 de enero de 2025 a las 19:52 UTC
- Hora editada: 31 de enero de 2025 a las 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SecretsManagerReadWrite

Descripción: Proporciona acceso de lectura/escritura a AWS Secrets Manager a través del. AWS Management Console Nota: esto excluye las acciones de IAM, así que combínelas con IAMFull Access si es necesario configurar la rotación.

`SecretsManagerReadWrite` es una política administrada de AWS.

Uso de la política

Puede asociar `SecretsManagerReadWrite` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 4 de abril de 2018 a las 18:05 UTC
- Hora de edición: 22 de febrero de 2024 a las 18:12 h UTC

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

Versión de la política

Versión de la política: v5 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*/*"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SecurityAudit

Descripción: la plantilla de auditoría de seguridad concede acceso para leer los metadatos de la configuración de seguridad. Sirve para el software que audita la configuración de una Cuenta de AWS.

`SecurityAudit` es una política administrada de AWS.

Uso de la política

Puede asociar `SecurityAudit` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora editada: 2 de julio de 2025 a las 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Versión de la política

Versión de la política: v52 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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: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:GetCustomModel",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "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:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "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:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "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:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "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:DescribePublishingDestination",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribeMalwareScans",
        "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:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "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*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
```

```
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensGroup",
        "s3:GetStorageLensConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListStorageLensGroups",
        "s3:ListJobs",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrants",
        "s3:ListStorageLensConfigurations",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:GetEncryptionConfiguration",
```

```
        "s3express:GetBucketPolicy",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3tables:ListTableBuckets",
        "s3tables:ListNamespaces",
        "s3tables:ListTables",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "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*",
        "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:DescribePermissionSet",
            "sso:DescribePermissionsPolicies",
            "sso:DescribeAccountAssignmentDeletionStatus",
            "sso:DescribeApplication",
            "sso:DescribeApplicationAssignment",
            "sso:DescribeApplicationProvider",
            "sso:DescribeInstance",
            "sso:DescribeInstanceAccessControlAttributeConfiguration",
            "sso:DescribePermissionSetProvisioningStatus",
            "sso:DescribeTrustedTokenIssuer",
            "sso:GetApplicationAccessScope",
            "sso:GetApplicationAssignmentConfiguration",
            "sso:GetApplicationAuthenticationMethod",
            "sso:GetApplicationGrant",
            "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:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SecurityLakeResourceManagementServiceRolePolicy

Descripción: Proporciona acceso para administrar los recursos creados por Security Lake.

`SecurityLakeResourceManagementServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2024 a las 22:10 UTC
- Hora editada: 14 de noviembre de 2024 a las 22:10 UTC

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

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "lambda:FunctionArn" :
 "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${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}"
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SecurityLakeServiceLinkedRole

Descripción: esta política concede permisos para operar el servicio Amazon Security Lake en su nombre

`SecurityLakeServiceLinkedRole` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 29 de noviembre de 2022 a las 14:03 UTC
- Hora de edición: 19 de abril de 2024 a las 16:00 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "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"
          ]
        }
      }
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServerMigration_ServiceRole

Descripción: Permisos que permiten al Servicio de migración de AWS servidores migrar VMs a EC2: permiten al Servicio de migración de servidores colocar los recursos migrados en la EC2 cuenta del cliente.

`ServerMigration_ServiceRole` es una política administrada de AWS.

Uso de la política

Puede asociar `ServerMigration_ServiceRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 11 de agosto de 2020 a las 20:41 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*/*"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServerMigrationConnector

Descripción: Permisos para permitir la migración AWS del conector de migración del servidor VMs a EC2. Permite la comunicación con el Servicio de migración de AWS servidores, el acceso de lectura y escritura a los buckets de S3 que comiencen por «sms-b-» y «import-to-ec2-», así como a los depósitos utilizados para actualizar el conector de migración de AWS servidores, registrar el conector de migración de AWS servidores y cargar las métricas en él. AWS AWS

`ServerMigrationConnector` es una política administrada de AWS.

Uso de la política

Puede asociar `ServerMigrationConnector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 24 de octubre de 2016 a las 21:45 UTC
- Hora de edición: 24 de octubre de 2016 a las 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServerMigrationServiceConsoleFullAccess

Descripción: permisos necesarios para usar todas las características de la Consola del Server Migration Service

`ServerMigrationServiceConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ServerMigrationServiceConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 9 de mayo de 2020 a las 17:18 UTC
- Hora de edición: 20 de julio de 2020 a las 22:00 UTC

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

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServerMigrationServiceLaunchRole

Descripción: Permisos que permiten al Servicio de Migración de AWS Servidores crear y actualizar AWS los recursos pertinentes en los del cliente Cuenta de AWS para lanzar los servidores y aplicaciones migrados.

`ServerMigrationServiceLaunchRole` es una política administrada de AWS.

Uso de la política

Puede asociar `ServerMigrationServiceLaunchRole` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 26 de noviembre de 2018 a las 19:53 UTC
- Hora de edición: 15 de octubre de 2020 a las 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServerMigrationServiceRoleForInstanceValidation

Descripción: Permisos para permitir que el AWS SMS ejecute el script de validación de datos utilizado y devuelva el script correcto o incorrecto al SMS

`ServerMigrationServiceRoleForInstanceValidation` es una política administrada de AWS.

Uso de la política

Puede asociar `ServerMigrationServiceRoleForInstanceValidation` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 20 de julio de 2020 a las 22:25 UTC
- Hora de edición: 20 de julio de 2020 a las 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServiceQuotasFullAccess

Descripción: proporciona acceso completo a Service Quotas

`ServiceQuotasFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ServiceQuotasFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2019 a las 15:44 UTC
- Hora de edición: 4 de febrero de 2021 a las 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Versión de la política

Versión de la política: v4 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
        }
      }
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServiceQuotasReadOnlyAccess

Descripción: proporciona acceso de solo lectura a Service Quotas

`ServiceQuotasReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ServiceQuotasReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 24 de junio de 2019 a las 15:31 UTC
- Hora de edición: 21 de diciembre de 2020 a las 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
      ],
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ServiceQuotasServiceRolePolicy

Descripción: permite a Service Quotas crear casos de soporte en su nombre

`ServiceQuotasServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 22 de mayo de 2019 a las 20:44 UTC
- Hora de edición: 24 de junio de 2019 a las 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SimpleWorkflowFullAccess

Descripción: proporciona acceso completo al servicio de configuración de Simple Workflow.

`SimpleWorkflowFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `SimpleWorkflowFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 6 de febrero de 2015 a las 18:41 UTC
- Hora de edición: 6 de febrero de 2015 a las 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SMSVoiceServiceRolePolicy

Descripción: Permite SMSVoice publicar métricas CloudWatch en su nombre

`SMSVoiceServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 14 de noviembre de 2024 a las 17:04 UTC
- Hora editada: 14 de noviembre de 2024 a las 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SplitCostAllocationDataServiceRolePolicy

Descripción: Permite que los datos de asignación de costos divididos recuperen la información de AWS las Organizaciones, si corresponde, y recopilen datos de telemetría para los servicios de datos de asignación de costos divididos que el cliente haya elegido.

`SplitCostAllocationDataServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 16 de abril de 2024 a las 16:05 h UTC
- Hora de edición: 16 de abril de 2024 a las 16:05 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
```

```
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SSMQuickSetupRolePolicy

Descripción: proporciona permiso para comprobar el estado de la configuración de Configuración rápida, garantizar el uso consistente de los parámetros y los recursos aprovisionados y corregir los recursos cuando se detecta una desviación.

`SSMQuickSetupRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 25 de junio de 2024 a las 15:20 h UTC
- Hora editada: 18 de noviembre de 2024 a las 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : [
        "*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SupportUser

Descripción: esta política otorga permisos para solucionar y resolver problemas en una Cuenta de AWS. Esta política también permite al usuario ponerse en contacto con el servicio de AWS asistencia para crear y gestionar casos.

`SupportUser` es una política administrada de AWS.

Uso de la política

Puede asociar `SupportUser` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:21 UTC
- Hora de edición: 25 de agosto de 2023 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Versión de la política

Versión de la política: v8 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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*",
        "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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

SystemAdministrator

Descripción: concede permisos de acceso completo necesarios para los recursos que las operaciones de desarrollo y aplicaciones precisan.

`SystemAdministrator` es una política administrada de AWS.

Uso de la política

Puede asociar `SystemAdministrator` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:23 UTC
- Hora editada: 11 de febrero de 2025 a las 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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",
        "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"
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

TranslateFullAccess

Descripción: proporciona acceso completo a Amazon Translate.

`TranslateFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `TranslateFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 27 de noviembre de 2018 a las 23:36 UTC
- Hora de edición: 8 de enero de 2020 a las 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

TranslateReadOnly

Descripción: proporciona acceso de solo lectura a Amazon Translate.

`TranslateReadOnly` es una política administrada de AWS.

Uso de la política

Puede asociar `TranslateReadOnly` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 29 de noviembre de 2017 a las 18:22 UTC
- Hora de edición: 24 de mayo de 2023 a las 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Versión de la política

Versión de la política: v7 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

ViewOnlyAccess

Descripción: Esta política otorga permisos para ver los recursos y los metadatos básicos en todos los AWS servicios.

`ViewOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `ViewOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: Política de funciones laborales
- Hora de creación: 10 de noviembre de 2016 a las 17:20 UTC
- Hora editada: 28 de mayo de 2025 a las 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Versión de la política

Versión de la política: v25 (predeterminada)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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:ListTagsForResource",
        "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",
        "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*",
        "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:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
```

```
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "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"
      ]
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

VMImportExportRoleForAWSConnector

Descripción: Política predeterminada para la función de servicio de importación y exportación de máquinas virtuales, para los clientes que utilizan el AWS conector. El servicio VM Import/Export asume una función con esta política para cumplir con las solicitudes de migración de máquinas virtuales desde el dispositivo virtual AWS Connector. (Tenga en cuenta que AWS Connector utiliza la política administrada AWSConnector «» para emitir solicitudes en nombre del cliente al servicio VM Import/Export). Ofrece la posibilidad de crear AMIs instantáneas de EBS, modificar los atributos de las instantáneas de EBS, realizar llamadas «Describe*» a los EC2 objetos y leer desde buckets de S3 que comiencen por «2». import-to-ec

`VMImportExportRoleForAWSConnector` es una política administrada de AWS.

Uso de la política

Puede asociar `VMImportExportRoleForAWSConnector` a los usuarios, grupos y roles.

Información de la política

- Tipo: política de rol de servicio
- Hora de creación: 3 de septiembre de 2015 a las 20:48 UTC
- Hora de edición: 3 de septiembre de 2015 a las 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

VPCLatticeFullAccess

Descripción: proporciona acceso completo a Amazon VPC Lattice y a los servicios de dependencia.

`VPCLatticeFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `VPCLatticeFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de marzo de 2023 a las 02:49 UTC
- Hora editada: 1 de diciembre de 2024 a las 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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"
    }
  ]
```

```
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

VPCLatticeReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a Amazon VPC Lattice a través de los AWS Management Console servicios de dependencia y acceso limitado a ellos.

`VPCLatticeReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `VPCLatticeReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 30 de marzo de 2023 a las 02:47 UTC
- Hora editada: 1 de diciembre de 2024 a las 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

VPCLatticeServicesInvokeAccess

Descripción: proporciona acceso para invocar los servicios de Amazon VPC Lattice.

`VPCLatticeServicesInvokeAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `VPCLatticeServicesInvokeAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 30 de marzo de 2023 a las 02:45 UTC
- Hora de edición: 30 de marzo de 2023 a las 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
```

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WAFLoggingServiceRolePolicy

Descripción: creación de rol vinculado al servicio para escribir los registros del cliente en un flujo de Firehose

`WAFLoggingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2018 a las 21:05 UTC
- Hora de edición: 24 de agosto de 2018 a las 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WAFRegionalLoggingServiceRolePolicy

Descripción: creación de rol vinculado al servicio para escribir los registros del cliente en un flujo de Firehose

`WAFRegionalLoggingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 24 de agosto de 2018 a las 18:40 UTC
- Hora de edición: 24 de agosto de 2018 a las 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WAFV2LoggingServiceRolePolicy

Descripción: Esta política crea un rol vinculado a un servicio que permite a AWS WAF escribir registros en Amazon Kinesis Data Firehose.

`WAFV2LoggingServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles.

Información de la política

- Tipo: política de rol vinculado a un servicio
- Hora de creación: 7 de noviembre de 2019 a las 00:40 UTC
- Hora de edición: 03 de junio de 2024 a las 17:29 h UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Versión de la política

Versión de la política: v3 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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" : "*"
    }
  ]
}
```

Más información

- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WellArchitectedConsoleFullAccess

Descripción: Proporciona acceso completo a la herramienta AWS Well-Architected a través del AWS Management Console

`WellArchitectedConsoleFullAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `WellArchitectedConsoleFullAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2018 a las 18:19 UTC
- Hora de edición: 29 de noviembre de 2018 a las 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WellArchitectedConsoleReadOnlyAccess

Descripción: Proporciona acceso de solo lectura a la herramienta Well-Architected mediante AWS el AWS Management Console

`WellArchitectedConsoleReadOnlyAccess` es una política administrada de AWS.

Uso de la política

Puede asociar `WellArchitectedConsoleReadOnlyAccess` a los usuarios, grupos y roles.

Información de la política

- Tipo: política gestionada AWS
- Hora de creación: 29 de noviembre de 2018 a las 18:21 UTC
- Hora de edición: 29 de junio de 2023 a las 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Versión de la política

Versión de la política: v2 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política JSON

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

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

WorkLinkServiceRolePolicy

Descripción: Permite el acceso Servicios de AWS y los recursos utilizados o gestionados por Amazon WorkLink

`WorkLinkServiceRolePolicy` es una política administrada de AWS.

Uso de la política

Puede asociar `WorkLinkServiceRolePolicy` a los usuarios, grupos y roles.

Información de la política

- Tipo: política AWS gestionada
- Hora de creación: 23 de enero de 2019 a las 19:03 UTC
- Hora de edición: 23 de enero de 2019 a las 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Versión de la política

Versión de la política: v1 (predeterminado)

La versión predeterminada de la política define qué permisos tendrá. Cuando un usuario o un rol con la política solicita el acceso a un AWS recurso, AWS comprueba la versión predeterminada de la política para determinar si permite la solicitud.

Documento de política 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-*"
    }
  ]
}
```

Más información

- Cree un conjunto de permisos mediante políticas AWS administradas en el Centro de identidades de IAM
- Adición y eliminación de permisos de identidad de IAM
- Conozca el control de versiones de las políticas de IAM
- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.