



参考指南

AWS 托管策略



AWS 托管策略: 参考指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS 托管策略？	1
了解策略参考页面	1
已弃用的 AWS 托管策略	2
AWS 托管策略	3
AccessAnalyzerServiceRolePolicy	44
使用此策略	44
策略详细信息	44
策略版本	44
JSON 策略文档	45
了解更多信息	47
AdministratorAccess	47
使用此策略	47
策略详细信息	47
策略版本	48
JSON 策略文档	48
了解更多信息	48
AdministratorAccess-Amplify	48
使用此策略	48
策略详细信息	48
策略版本	49
JSON 策略文档	49
了解更多信息	59
AdministratorAccess-AWSElasticBeanstalk	59
使用此策略	60
策略详细信息	60
策略版本	60
JSON 策略文档	60
了解更多信息	68
AlexaForBusinessDeviceSetup	68
使用此策略	69
策略详细信息	69
策略版本	69
JSON 策略文档	69
了解更多信息	70

AlexaForBusinessFullAccess	70
使用此策略	70
策略详细信息	70
策略版本	70
JSON 策略文档	71
了解更多信息	72
AlexaForBusinessGatewayExecution	72
使用此策略	72
策略详细信息	72
策略版本	73
JSON 策略文档	73
了解更多信息	74
AlexaForBusinessLifesizeDelegatedAccessPolicy	74
使用此策略	74
策略详细信息	74
策略版本	74
JSON 策略文档	74
了解更多信息	77
AlexaForBusinessNetworkProfileServicePolicy	77
使用此策略	77
策略详细信息	77
策略版本	77
JSON 策略文档	78
了解更多信息	78
AlexaForBusinessPolyDelegatedAccessPolicy	78
使用此策略	79
策略详细信息	79
策略版本	79
JSON 策略文档	79
了解更多信息	81
AlexaForBusinessReadOnlyAccess	81
使用此策略	81
策略详细信息	81
策略版本	81
JSON 策略文档	82
了解更多信息	82

AmazonAPIGatewayAdministrator	82
使用此策略	82
策略详细信息	83
策略版本	83
JSON 策略文档	83
了解更多信息	83
AmazonAPIGatewayInvokeFullAccess	84
使用此策略	84
策略详细信息	84
策略版本	84
JSON 策略文档	84
了解更多信息	85
AmazonAPIGatewayPushToCloudWatchLogs	85
使用此策略	85
策略详细信息	85
策略版本	85
JSON 策略文档	85
了解更多信息	86
AmazonAppFlowFullAccess	86
使用此策略	86
策略详细信息	86
策略版本	87
JSON 策略文档	87
了解更多信息	89
AmazonAppFlowReadOnlyAccess	90
使用此策略	90
策略详细信息	90
策略版本	90
JSON 策略文档	90
了解更多信息	91
AmazonAppStreamFullAccess	91
使用此策略	91
策略详细信息	91
策略版本	91
JSON 策略文档	92
了解更多信息	93

AmazonAppStreamPCAAccess	94
使用此策略	94
策略详细信息	94
策略版本	94
JSON 策略文档	94
了解更多信息	95
AmazonAppStreamReadOnlyAccess	95
使用此策略	95
策略详细信息	95
策略版本	95
JSON 策略文档	96
了解更多信息	96
AmazonAppStreamServiceAccess	96
使用此策略	96
策略详细信息	96
策略版本	97
JSON 策略文档	97
了解更多信息	98
AmazonAthenaFullAccess	98
使用此策略	98
策略详细信息	98
策略版本	99
JSON 策略文档	99
了解更多信息	102
AmazonAugmentedAIFullAccess	102
使用此策略	103
策略详细信息	103
策略版本	103
JSON 策略文档	103
了解更多信息	104
AmazonAugmentedAIHumanLoopFullAccess	104
使用此策略	104
策略详细信息	104
策略版本	105
JSON 策略文档	105
了解更多信息	105

AmazonAugmentedAllIntegratedAPIAccess	105
使用此策略	106
策略详细信息	106
策略版本	106
JSON 策略文档	106
了解更多信息	107
AmazonBedrockFullAccess	108
使用此策略	108
策略详细信息	108
策略版本	108
JSON 策略文档	108
了解更多信息	109
AmazonBedrockReadOnly	110
使用此策略	110
策略详细信息	110
策略版本	110
JSON 策略文档	110
了解更多信息	111
AmazonBraketFullAccess	111
使用此策略	111
策略详细信息	111
策略版本	111
JSON 策略文档	112
了解更多信息	116
AmazonBraketJobsExecutionPolicy	116
使用此策略	116
策略详细信息	116
策略版本	116
JSON 策略文档	117
了解更多信息	119
AmazonBraketServiceRolePolicy	119
使用此策略	119
策略详细信息	120
策略版本	120
JSON 策略文档	120
了解更多信息	121

AmazonChimeFullAccess	121
使用此策略	121
策略详细信息	121
策略版本	121
JSON 策略文档	121
了解更多信息	123
AmazonChimeReadOnly	124
使用此策略	124
策略详细信息	124
策略版本	124
JSON 策略文档	124
了解更多信息	125
AmazonChimeSDK	125
使用此策略	125
策略详细信息	125
策略版本	125
JSON 策略文档	126
了解更多信息	127
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	127
使用此策略	127
策略详细信息	127
策略版本	127
JSON 策略文档	127
了解更多信息	129
AmazonChimeSDKMessagingServiceRolePolicy	129
使用此策略	129
策略详细信息	129
策略版本	129
JSON 策略文档	129
了解更多信息	130
AmazonChimeServiceRolePolicy	130
使用此策略	131
策略详细信息	131
策略版本	131
JSON 策略文档	131
了解更多信息	132

AmazonChimeTranscriptionServiceLinkedRolePolicy	132
使用此策略	132
策略详细信息	132
策略版本	132
JSON 策略文档	132
了解更多信息	133
AmazonChimeUserManagement	133
使用此策略	133
策略详细信息	133
策略版本	133
JSON 策略文档	134
了解更多信息	135
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	135
使用此策略	135
策略详细信息	135
策略版本	135
JSON 策略文档	136
了解更多信息	137
AmazonCloudDirectoryFullAccess	138
使用此策略	138
策略详细信息	138
策略版本	138
JSON 策略文档	138
了解更多信息	139
AmazonCloudDirectoryReadOnlyAccess	139
使用此策略	139
策略详细信息	139
策略版本	139
JSON 策略文档	139
了解更多信息	140
AmazonCloudWatchEvidentlyFullAccess	140
使用此策略	140
策略详细信息	140
策略版本	141
JSON 策略文档	141
了解更多信息	143

AmazonCloudWatchEvidentlyReadOnlyAccess	143
使用此策略	144
策略详细信息	144
策略版本	144
JSON 策略文档	144
了解更多信息	145
AmazonCloudWatchEvidentlyServiceRolePolicy	145
使用此策略	145
策略详细信息	145
策略版本	145
JSON 策略文档	145
了解更多信息	147
AmazonCloudWatchRUMFullAccess	147
使用此策略	147
策略详细信息	147
策略版本	147
JSON 策略文档	148
了解更多信息	150
AmazonCloudWatchRUMReadOnlyAccess	150
使用此策略	150
策略详细信息	150
策略版本	151
JSON 策略文档	151
了解更多信息	151
AmazonCloudWatchRUMServiceRolePolicy	152
使用此策略	152
策略详细信息	152
策略版本	152
JSON 策略文档	152
了解更多信息	153
AmazonCodeCatalystFullAccess	153
使用此策略	153
策略详细信息	153
策略版本	154
JSON 策略文档	154
了解更多信息	155

AmazonCodeCatalystReadOnlyAccess	155
使用此策略	155
策略详细信息	155
策略版本	155
JSON 策略文档	155
了解更多信息	156
AmazonCodeCatalystSupportAccess	156
使用此策略	156
策略详细信息	156
策略版本	156
JSON 策略文档	157
了解更多信息	157
AmazonCodeGuruProfilerAgentAccess	158
使用此策略	158
策略详细信息	158
策略版本	158
JSON 策略文档	158
了解更多信息	159
AmazonCodeGuruProfilerFullAccess	159
使用此策略	159
策略详细信息	159
策略版本	159
JSON 策略文档	159
了解更多信息	160
AmazonCodeGuruProfilerReadOnlyAccess	160
使用此策略	160
策略详细信息	161
策略版本	161
JSON 策略文档	161
了解更多信息	161
AmazonCodeGuruReviewerFullAccess	162
使用此策略	162
策略详细信息	162
策略版本	162
JSON 策略文档	162
了解更多信息	165

AmazonCodeGuruReviewerReadOnlyAccess	165
使用此策略	165
策略详细信息	165
策略版本	165
JSON 策略文档	166
了解更多信息	166
AmazonCodeGuruReviewerServiceRolePolicy	166
使用此策略	166
策略详细信息	167
策略版本	167
JSON 策略文档	167
了解更多信息	169
AmazonCodeGuruSecurityFullAccess	169
使用此策略	169
策略详细信息	169
策略版本	170
JSON 策略文档	170
了解更多信息	170
AmazonCodeGuruSecurityScanAccess	170
使用此策略	170
策略详细信息	171
策略版本	171
JSON 策略文档	171
了解更多信息	171
AmazonCognitoDeveloperAuthenticatedIdentities	172
使用此策略	172
策略详细信息	172
策略版本	172
JSON 策略文档	172
了解更多信息	173
AmazonCognitoIdpEmailServiceRolePolicy	173
使用此策略	173
策略详细信息	173
策略版本	173
JSON 策略文档	174
了解更多信息	174

AmazonCognitoDpServiceRolePolicy	174
使用此策略	174
策略详细信息	174
策略版本	175
JSON 策略文档	175
了解更多信息	175
AmazonCognitoPowerUser	175
使用此策略	176
策略详细信息	176
策略版本	176
JSON 策略文档	176
了解更多信息	177
AmazonCognitoReadOnly	178
使用此策略	178
策略详细信息	178
策略版本	178
JSON 策略文档	178
了解更多信息	179
AmazonCognitoUnAuthedIdentitiesSessionPolicy	179
使用此策略	179
策略详细信息	179
策略版本	180
JSON 策略文档	180
了解更多信息	180
AmazonCognitoUnauthenticatedIdentities	181
使用此策略	181
策略详细信息	181
策略版本	181
JSON 策略文档	181
了解更多信息	182
AmazonConnect_FullAccess	182
使用此策略	182
策略详细信息	182
策略版本	182
JSON 策略文档	183
了解更多信息	185

AmazonConnectCampaignsServiceLinkedRolePolicy	185
使用此策略	185
策略详细信息	186
策略版本	186
JSON 策略文档	186
了解更多信息	187
AmazonConnectReadOnlyAccess	187
使用此策略	187
策略详细信息	187
策略版本	187
JSON 策略文档	187
了解更多信息	188
AmazonConnectServiceLinkedRolePolicy	188
使用此策略	188
策略详细信息	188
策略版本	189
JSON 策略文档	189
了解更多信息	194
AmazonConnectSynchronizationServiceRolePolicy	194
使用此策略	194
策略详细信息	194
策略版本	195
JSON 策略文档	195
了解更多信息	197
AmazonConnectVoiceIDFullAccess	197
使用此策略	197
策略详细信息	197
策略版本	197
JSON 策略文档	197
了解更多信息	198
AmazonDataZoneDomainExecutionRolePolicy	198
使用此策略	198
策略详细信息	198
策略版本	199
JSON 策略文档	199
了解更多信息	202

AmazonDataZoneEnvironmentRolePermissionsBoundary	202
使用此策略	202
策略详细信息	202
策略版本	202
JSON 策略文档	202
了解更多信息	215
AmazonDataZoneFullAccess	216
使用此策略	216
策略详细信息	216
策略版本	216
JSON 策略文档	216
了解更多信息	220
AmazonDataZoneFullUserAccess	220
使用此策略	220
策略详细信息	220
策略版本	220
JSON 策略文档	220
了解更多信息	223
AmazonDataZoneGlueManageAccessRolePolicy	223
使用此策略	224
策略详细信息	224
策略版本	224
JSON 策略文档	224
了解更多信息	229
AmazonDataZonePortalFullAccessPolicy	229
使用此策略	229
策略详细信息	229
策略版本	230
JSON 策略文档	230
了解更多信息	230
AmazonDataZonePreviewConsoleFullAccess	230
使用此策略	231
策略详细信息	231
策略版本	231
JSON 策略文档	231
了解更多信息	233

AmazonDataZoneProjectDeploymentPermissionsBoundary	233
使用此策略	233
策略详细信息	233
策略版本	234
JSON 策略文档	234
了解更多信息	242
AmazonDataZoneProjectRolePermissionsBoundary	242
使用此策略	242
策略详细信息	242
策略版本	242
JSON 策略文档	243
了解更多信息	250
AmazonDataZoneRedshiftGlueProvisioningPolicy	250
使用此策略	250
策略详细信息	250
策略版本	250
JSON 策略文档	251
了解更多信息	258
AmazonDataZoneRedshiftManageAccessRolePolicy	259
使用此策略	259
策略详细信息	259
策略版本	259
JSON 策略文档	259
了解更多信息	261
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary	262
使用此策略	262
策略详细信息	262
策略版本	262
JSON 策略文档	262
了解更多信息	289
AmazonDataZoneSageMakerManageAccessRolePolicy	290
使用此策略	290
策略详细信息	290
策略版本	290
JSON 策略文档	290
了解更多信息	295

AmazonDataZoneSageMakerProvisioningRolePolicy	295
使用此策略	295
策略详细信息	295
策略版本	295
JSON 策略文档	296
了解更多信息	300
AmazonDetectiveFullAccess	300
使用此策略	301
策略详细信息	301
策略版本	301
JSON 策略文档	301
了解更多信息	302
AmazonDetectiveInvestigatorAccess	302
使用此策略	302
策略详细信息	302
策略版本	303
JSON 策略文档	303
了解更多信息	304
AmazonDetectiveMemberAccess	305
使用此策略	305
策略详细信息	305
策略版本	305
JSON 策略文档	305
了解更多信息	306
AmazonDetectiveOrganizationsAccess	306
使用此策略	306
策略详细信息	306
策略版本	306
JSON 策略文档	307
了解更多信息	308
AmazonDetectiveServiceLinkedRolePolicy	308
使用此策略	309
策略详细信息	309
策略版本	309
JSON 策略文档	309
了解更多信息	309

AmazonDevOpsGuruConsoleFullAccess	310
使用此策略	310
策略详细信息	310
策略版本	310
JSON 策略文档	310
了解更多信息	313
AmazonDevOpsGuruFullAccess	313
使用此策略	313
策略详细信息	313
策略版本	313
JSON 策略文档	313
了解更多信息	316
AmazonDevOpsGuruOrganizationsAccess	316
使用此策略	316
策略详细信息	316
策略版本	316
JSON 策略文档	316
了解更多信息	318
AmazonDevOpsGuruReadOnlyAccess	318
使用此策略	318
策略详细信息	318
策略版本	318
JSON 策略文档	318
了解更多信息	320
AmazonDevOpsGuruServiceRolePolicy	321
使用此策略	321
策略详细信息	321
策略版本	321
JSON 策略文档	321
了解更多信息	325
AmazonDMSCloudWatchLogsRole	325
使用此策略	325
策略详细信息	326
策略版本	326
JSON 策略文档	326
了解更多信息	327

AmazonDMSRedshiftS3Role	328
使用此策略	328
策略详细信息	328
策略版本	328
JSON 策略文档	328
了解更多信息	329
AmazonDMSVPCManagementRole	329
使用此策略	329
策略详细信息	329
策略版本	330
JSON 策略文档	330
了解更多信息	330
AmazonDocDB-ElasticServiceRolePolicy	331
使用此策略	331
策略详细信息	331
策略版本	331
JSON 策略文档	331
了解更多信息	332
AmazonDocDBConsoleFullAccess	332
使用此策略	332
策略详细信息	332
策略版本	332
JSON 策略文档	333
了解更多信息	337
AmazonDocDBElasticFullAccess	337
使用此策略	337
策略详细信息	337
策略版本	337
JSON 策略文档	338
了解更多信息	341
AmazonDocDBElasticReadOnlyAccess	341
使用此策略	341
策略详细信息	341
策略版本	341
JSON 策略文档	341
了解更多信息	342

AmazonDocDBFullAccess	342
使用此策略	342
策略详细信息	343
策略版本	343
JSON 策略文档	343
了解更多信息	346
AmazonDocDBReadOnlyAccess	346
使用此策略	346
策略详细信息	346
策略版本	346
JSON 策略文档	346
了解更多信息	348
AmazonDRSVPCManagement	348
使用此策略	349
策略详细信息	349
策略版本	349
JSON 策略文档	349
了解更多信息	350
AmazonDynamoDBFullAccess	350
使用此策略	350
策略详细信息	350
策略版本	350
JSON 策略文档	351
了解更多信息	353
AmazonDynamoDBFullAccesswithDataPipeline	353
使用此策略	354
策略详细信息	354
策略版本	354
JSON 策略文档	354
了解更多信息	356
AmazonDynamoDBReadOnlyAccess	356
使用此策略	356
策略详细信息	357
策略版本	357
JSON 策略文档	357
了解更多信息	359

AmazonEBSCSIDriverPolicy	359
使用此策略	359
策略详细信息	359
策略版本	359
JSON 策略文档	359
了解更多信息	363
AmazonEC2ContainerRegistryFullAccess	363
使用此策略	363
策略详细信息	363
策略版本	363
JSON 策略文档	363
了解更多信息	364
AmazonEC2ContainerRegistryPowerUser	364
使用此策略	364
策略详细信息	365
策略版本	365
JSON 策略文档	365
了解更多信息	366
AmazonEC2ContainerRegistryReadOnly	366
使用此策略	366
策略详细信息	366
策略版本	366
JSON 策略文档	366
了解更多信息	367
AmazonEC2ContainerServiceAutoscaleRole	367
使用此策略	367
策略详细信息	368
策略版本	368
JSON 策略文档	368
了解更多信息	369
AmazonEC2ContainerServiceEventsRole	369
使用此策略	369
策略详细信息	369
策略版本	369
JSON 策略文档	370
了解更多信息	371

AmazonEC2ContainerServiceforEC2Role	371
使用此策略	371
策略详细信息	371
策略版本	371
JSON 策略文档	371
了解更多信息	372
AmazonEC2ContainerServiceRole	373
使用此策略	373
策略详细信息	373
策略版本	373
JSON 策略文档	373
了解更多信息	374
AmazonEC2FullAccess	374
使用此策略	374
策略详细信息	374
策略版本	374
JSON 策略文档	375
了解更多信息	376
AmazonEC2ReadOnlyAccess	376
使用此策略	376
策略详细信息	376
策略版本	376
JSON 策略文档	376
了解更多信息	377
AmazonEC2RoleforAWSCodeDeploy	377
使用此策略	378
策略详细信息	378
策略版本	378
JSON 策略文档	378
了解更多信息	378
AmazonEC2RoleforAWSCodeDeployLimited	379
使用此策略	379
策略详细信息	379
策略版本	379
JSON 策略文档	379
了解更多信息	380

AmazonEC2RoleforDataPipelineRole	380
使用此策略	380
策略详细信息	381
策略版本	381
JSON 策略文档	381
了解更多信息	382
AmazonEC2RoleforSSM	382
使用此策略	382
策略详细信息	382
策略版本	382
JSON 策略文档	383
了解更多信息	385
AmazonEC2RolePolicyForLaunchWizard	385
使用此策略	385
策略详细信息	385
策略版本	386
JSON 策略文档	386
了解更多信息	390
AmazonEC2SpotFleetAutoscaleRole	390
使用此策略	390
策略详细信息	390
策略版本	390
JSON 策略文档	390
了解更多信息	391
AmazonEC2SpotFleetTaggingRole	392
使用此策略	392
策略详细信息	392
策略版本	392
JSON 策略文档	392
了解更多信息	393
AmazonECS_FullAccess	394
使用此策略	394
策略详细信息	394
策略版本	394
JSON 策略文档	394
了解更多信息	400

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	400
使用此策略	400
策略详细信息	400
策略版本	400
JSON 策略文档	401
了解更多信息	403
AmazonECSInfrastructureRolePolicyForVolumes	403
使用此策略	403
策略详细信息	403
策略版本	403
JSON 策略文档	404
了解更多信息	405
AmazonECSServiceRolePolicy	406
使用此策略	406
策略详细信息	406
策略版本	406
JSON 策略文档	406
了解更多信息	411
AmazonECSTaskExecutionRolePolicy	411
使用此策略	411
策略详细信息	411
策略版本	412
JSON 策略文档	412
了解更多信息	412
AmazonEFSCSIDriverPolicy	413
使用此策略	413
策略详细信息	413
策略版本	413
JSON 策略文档	413
了解更多信息	415
AmazonEKS_CNI_Policy	415
使用此策略	415
策略详细信息	415
策略版本	415
JSON 策略文档	416
了解更多信息	416

AmazonEKSClusterPolicy	417
使用此策略	417
策略详细信息	417
策略版本	417
JSON 策略文档	417
了解更多信息	419
AmazonEKSConectorServiceRolePolicy	419
使用此策略	420
策略详细信息	420
策略版本	420
JSON 策略文档	420
了解更多信息	422
AmazonEKSFargatePodExecutionRolePolicy	422
使用此策略	422
策略详细信息	422
策略版本	422
JSON 策略文档	423
了解更多信息	423
AmazonEKSFForFargateServiceRolePolicy	423
使用此策略	423
策略详细信息	424
策略版本	424
JSON 策略文档	424
了解更多信息	425
AmazonEKSLocalOutpostClusterPolicy	425
使用此策略	425
策略详细信息	425
策略版本	425
JSON 策略文档	425
了解更多信息	427
AmazonEKSLocalOutpostServiceRolePolicy	427
使用此策略	427
策略详细信息	428
策略版本	428
JSON 策略文档	428
了解更多信息	434

AmazonEKSServicePolicy	434
使用此策略	434
策略详细信息	434
策略版本	434
JSON 策略文档	434
了解更多信息	436
AmazonEKSServiceRolePolicy	436
使用此策略	436
策略详细信息	436
策略版本	437
JSON 策略文档	437
了解更多信息	439
AmazonEKSVPCResourceController	439
使用此策略	439
策略详细信息	439
策略版本	440
JSON 策略文档	440
了解更多信息	441
AmazonEKSWorkerNodePolicy	441
使用此策略	441
策略详细信息	441
策略版本	441
JSON 策略文档	441
了解更多信息	442
AmazonElastiCacheFullAccess	442
使用此策略	442
策略详细信息	442
策略版本	443
JSON 策略文档	443
了解更多信息	446
AmazonElastiCacheReadOnlyAccess	446
使用此策略	446
策略详细信息	446
策略版本	447
JSON 策略文档	447
了解更多信息	447

AmazonElasticContainerRegistryPublicFullAccess	447
使用此策略	448
策略详细信息	448
策略版本	448
JSON 策略文档	448
了解更多信息	448
AmazonElasticContainerRegistryPublicPowerUser	449
使用此策略	449
策略详细信息	449
策略版本	449
JSON 策略文档	449
了解更多信息	450
AmazonElasticContainerRegistryPublicReadOnly	450
使用此策略	450
策略详细信息	450
策略版本	451
JSON 策略文档	451
了解更多信息	451
AmazonElasticFileSystemClientFullAccess	452
使用此策略	452
策略详细信息	452
策略版本	452
JSON 策略文档	452
了解更多信息	453
AmazonElasticFileSystemClientReadOnlyAccess	453
使用此策略	453
策略详细信息	453
策略版本	453
JSON 策略文档	453
了解更多信息	454
AmazonElasticFileSystemClientReadWriteAccess	454
使用此策略	454
策略详细信息	454
策略版本	454
JSON 策略文档	455
了解更多信息	455

AmazonElasticFileSystemFullAccess	455
使用此策略	455
策略详细信息	455
策略版本	456
JSON 策略文档	456
了解更多信息	458
AmazonElasticFileSystemReadOnlyAccess	458
使用此策略	458
策略详细信息	458
策略版本	458
JSON 策略文档	458
了解更多信息	459
AmazonElasticFileSystemServiceRolePolicy	459
使用此策略	460
策略详细信息	460
策略版本	460
JSON 策略文档	460
了解更多信息	462
AmazonElasticFileSystemsUtils	462
使用此策略	462
策略详细信息	463
策略版本	463
JSON 策略文档	463
了解更多信息	465
AmazonElasticMapReduceEditorsRole	465
使用此策略	465
策略详细信息	465
策略版本	465
JSON 策略文档	466
了解更多信息	467
AmazonElasticMapReduceforAutoScalingRole	467
使用此策略	467
策略详细信息	467
策略版本	467
JSON 策略文档	468
了解更多信息	468

AmazonElasticMapReduceforEC2Role	468
使用此策略	468
策略详细信息	468
策略版本	469
JSON 策略文档	469
了解更多信息	470
AmazonElasticMapReduceFullAccess	470
使用此策略	471
策略详细信息	471
策略版本	471
JSON 策略文档	471
了解更多信息	473
AmazonElasticMapReducePlacementGroupPolicy	473
使用此策略	473
策略详细信息	473
策略版本	473
JSON 策略文档	473
了解更多信息	474
AmazonElasticMapReduceReadOnlyAccess	474
使用此策略	474
策略详细信息	474
策略版本	475
JSON 策略文档	475
了解更多信息	475
AmazonElasticMapReduceRole	476
使用此策略	476
策略详细信息	476
策略版本	476
JSON 策略文档	476
了解更多信息	478
AmazonElasticsearchServiceRolePolicy	479
使用此策略	479
策略详细信息	479
策略版本	479
JSON 策略文档	479
了解更多信息	482

AmazonElasticTranscoder_FullAccess	482
使用此策略	482
策略详细信息	482
策略版本	483
JSON 策略文档	483
了解更多信息	484
AmazonElasticTranscoder_JobsSubmitter	484
使用此策略	484
策略详细信息	484
策略版本	484
JSON 策略文档	484
了解更多信息	485
AmazonElasticTranscoder_ReadOnlyAccess	485
使用此策略	485
策略详细信息	485
策略版本	486
JSON 策略文档	486
了解更多信息	486
AmazonElasticTranscoderRole	486
使用此策略	487
策略详细信息	487
策略版本	487
JSON 策略文档	487
了解更多信息	488
AmazonEMRCleanupPolicy	488
使用此策略	488
策略详细信息	488
策略版本	488
JSON 策略文档	489
了解更多信息	489
AmazonEMRContainersServiceRolePolicy	489
使用此策略	490
策略详细信息	490
策略版本	490
JSON 策略文档	490
了解更多信息	491

AmazonEMRFullAccessPolicy_v2	491
使用此策略	492
策略详细信息	492
策略版本	492
JSON 策略文档	492
了解更多信息	495
AmazonEMRReadOnlyAccessPolicy_v2	496
使用此策略	496
策略详细信息	496
策略版本	496
JSON 策略文档	496
了解更多信息	497
AmazonEMRServerlessServiceRolePolicy	497
使用此策略	498
策略详细信息	498
策略版本	498
JSON 策略文档	498
了解更多信息	499
AmazonEMRServicePolicy_v2	499
使用此策略	499
策略详细信息	499
策略版本	500
JSON 策略文档	500
了解更多信息	507
AmazonESCognitoAccess	508
使用此策略	508
策略详细信息	508
策略版本	508
JSON 策略文档	508
了解更多信息	509
AmazonESFullAccess	509
使用此策略	509
策略详细信息	510
策略版本	510
JSON 策略文档	510
了解更多信息	510

AmazonESReadOnlyAccess	511
使用此策略	511
策略详细信息	511
策略版本	511
JSON 策略文档	511
了解更多信息	512
AmazonEventBridgeApiDestinationsServiceRolePolicy	512
使用此策略	512
策略详细信息	512
策略版本	512
JSON 策略文档	512
了解更多信息	513
AmazonEventBridgeFullAccess	513
使用此策略	513
策略详细信息	513
策略版本	513
JSON 策略文档	514
了解更多信息	516
AmazonEventBridgePipesFullAccess	516
使用此策略	516
策略详细信息	516
策略版本	516
JSON 策略文档	516
了解更多信息	517
AmazonEventBridgePipesOperatorAccess	517
使用此策略	517
策略详细信息	518
策略版本	518
JSON 策略文档	518
了解更多信息	518
AmazonEventBridgePipesReadOnlyAccess	519
使用此策略	519
策略详细信息	519
策略版本	519
JSON 策略文档	519
了解更多信息	520

AmazonEventBridgeReadOnlyAccess	520
使用此策略	520
策略详细信息	520
策略版本	520
JSON 策略文档	521
了解更多信息	522
AmazonEventBridgeSchedulerFullAccess	522
使用此策略	522
策略详细信息	522
策略版本	523
JSON 策略文档	523
了解更多信息	523
AmazonEventBridgeSchedulerReadOnlyAccess	524
使用此策略	524
策略详细信息	524
策略版本	524
JSON 策略文档	524
了解更多信息	525
AmazonEventBridgeSchemasFullAccess	525
使用此策略	525
策略详细信息	525
策略版本	525
JSON 策略文档	526
了解更多信息	526
AmazonEventBridgeSchemasReadOnlyAccess	527
使用此策略	527
策略详细信息	527
策略版本	527
JSON 策略文档	527
了解更多信息	528
AmazonEventBridgeSchemasServiceRolePolicy	528
使用此策略	528
策略详细信息	528
策略版本	529
JSON 策略文档	529
了解更多信息	529

AmazonFISServiceRolePolicy	529
使用此策略	530
策略详细信息	530
策略版本	530
JSON 策略文档	530
了解更多信息	532
AmazonForecastFullAccess	532
使用此策略	532
策略详细信息	532
策略版本	532
JSON 策略文档	532
了解更多信息	533
AmazonFraudDetectorFullAccessPolicy	533
使用此策略	533
策略详细信息	534
策略版本	534
JSON 策略文档	534
了解更多信息	535
AmazonFreeRTOSFullAccess	535
使用此策略	535
策略详细信息	536
策略版本	536
JSON 策略文档	536
了解更多信息	536
AmazonFreeRTOSOTAUpdate	537
使用此策略	537
策略详细信息	537
策略版本	537
JSON 策略文档	537
了解更多信息	539
AmazonFSxConsoleFullAccess	539
使用此策略	539
策略详细信息	539
策略版本	539
JSON 策略文档	539
了解更多信息	543

AmazonFSxConsoleReadOnlyAccess	543
使用此策略	543
策略详细信息	543
策略版本	543
JSON 策略文档	544
了解更多信息	544
AmazonFSxFullAccess	545
使用此策略	545
策略详细信息	545
策略版本	545
JSON 策略文档	545
了解更多信息	549
AmazonFSxReadOnlyAccess	549
使用此策略	550
策略详细信息	550
策略版本	550
JSON 策略文档	550
了解更多信息	550
AmazonFSxServiceRolePolicy	551
使用此策略	551
策略详细信息	551
策略版本	551
JSON 策略文档	551
了解更多信息	554
AmazonGlacierFullAccess	554
使用此策略	554
策略详细信息	554
策略版本	555
JSON 策略文档	555
了解更多信息	555
AmazonGlacierReadOnlyAccess	555
使用此策略	555
策略详细信息	555
策略版本	556
JSON 策略文档	556
了解更多信息	556

AmazonGrafanaAthenaAccess	557
使用此策略	557
策略详细信息	557
策略版本	557
JSON 策略文档	557
了解更多信息	559
AmazonGrafanaCloudWatchAccess	559
使用此策略	559
策略详细信息	560
策略版本	560
JSON 策略文档	560
了解更多信息	561
AmazonGrafanaRedshiftAccess	561
使用此策略	562
策略详细信息	562
策略版本	562
JSON 策略文档	562
了解更多信息	563
AmazonGrafanaServiceLinkedRolePolicy	564
使用此策略	564
策略详细信息	564
策略版本	564
JSON 策略文档	564
了解更多信息	565
AmazonGuardDutyFullAccess	566
使用此策略	566
策略详细信息	566
策略版本	566
JSON 策略文档	566
了解更多信息	568
AmazonGuardDutyMalwareProtectionServiceRolePolicy	568
使用此策略	568
策略详细信息	568
策略版本	568
JSON 策略文档	569
了解更多信息	573

AmazonGuardDutyReadOnlyAccess	573
使用此策略	573
策略详细信息	573
策略版本	574
JSON 策略文档	574
了解更多信息	574
AmazonGuardDutyServiceRolePolicy	575
使用此策略	575
策略详细信息	575
策略版本	575
JSON 策略文档	575
了解更多信息	581
AmazonHealthLakeFullAccess	581
使用此策略	582
策略详细信息	582
策略版本	582
JSON 策略文档	582
了解更多信息	583
AmazonHealthLakeReadOnlyAccess	583
使用此策略	583
策略详细信息	583
策略版本	583
JSON 策略文档	584
了解更多信息	584
AmazonHoneycodeFullAccess	584
使用此策略	584
策略详细信息	585
策略版本	585
JSON 策略文档	585
了解更多信息	585
AmazonHoneycodeReadOnlyAccess	586
使用此策略	586
策略详细信息	586
策略版本	586
JSON 策略文档	586
了解更多信息	587

AmazonHoneycodeServiceRolePolicy	587
使用此策略	587
策略详细信息	587
策略版本	587
JSON 策略文档	587
了解更多信息	588
AmazonHoneycodeTeamAssociationFullAccess	588
使用此策略	588
策略详细信息	588
策略版本	588
JSON 策略文档	589
了解更多信息	589
AmazonHoneycodeTeamAssociationReadOnlyAccess	589
使用此策略	589
策略详细信息	589
策略版本	590
JSON 策略文档	590
了解更多信息	590
AmazonHoneycodeWorkbookFullAccess	590
使用此策略	591
策略详细信息	591
策略版本	591
JSON 策略文档	591
了解更多信息	592
AmazonHoneycodeWorkbookReadOnlyAccess	592
使用此策略	592
策略详细信息	592
策略版本	592
JSON 策略文档	592
了解更多信息	593
AmazonInspector2AgentlessServiceRolePolicy	593
使用此策略	593
策略详细信息	593
策略版本	594
JSON 策略文档	594
了解更多信息	597

AmazonInspector2FullAccess	598
使用此策略	598
策略详细信息	598
策略版本	598
JSON 策略文档	598
了解更多信息	599
AmazonInspector2ManagedCisPolicy	600
使用此策略	600
策略详细信息	600
策略版本	600
JSON 策略文档	600
了解更多信息	601
AmazonInspector2ReadOnlyAccess	601
使用此策略	601
策略详细信息	601
策略版本	601
JSON 策略文档	601
了解更多信息	602
AmazonInspector2ServiceRolePolicy	602
使用此策略	602
策略详细信息	603
策略版本	603
JSON 策略文档	603
了解更多信息	609
AmazonInspectorFullAccess	609
使用此策略	610
策略详细信息	610
策略版本	610
JSON 策略文档	610
了解更多信息	611
AmazonInspectorReadOnlyAccess	611
使用此策略	611
策略详细信息	612
策略版本	612
JSON 策略文档	612
了解更多信息	612

AmazonInspectorServiceRolePolicy	613
使用此策略	613
策略详细信息	613
策略版本	613
JSON 策略文档	613
了解更多信息	615
AmazonKendraFullAccess	615
使用此策略	615
策略详细信息	615
策略版本	615
JSON 策略文档	615
了解更多信息	617
AmazonKendraReadOnlyAccess	617
使用此策略	618
策略详细信息	618
策略版本	618
JSON 策略文档	618
了解更多信息	618
AmazonKeyspacesFullAccess	619
使用此策略	619
策略详细信息	619
策略版本	619
JSON 策略文档	619
了解更多信息	621
AmazonKeyspacesReadOnlyAccess	621
使用此策略	621
策略详细信息	622
策略版本	622
JSON 策略文档	622
了解更多信息	623
AmazonKeyspacesReadOnlyAccess_v2	623
使用此策略	623
策略详细信息	623
策略版本	623
JSON 策略文档	623
了解更多信息	624

AmazonKinesisAnalyticsFullAccess	625
使用此策略	625
策略详细信息	625
策略版本	625
JSON 策略文档	625
了解更多信息	627
AmazonKinesisAnalyticsReadOnly	627
使用此策略	627
策略详细信息	627
策略版本	627
JSON 策略文档	627
了解更多信息	629
AmazonKinesisFirehoseFullAccess	629
使用此策略	629
策略详细信息	629
策略版本	629
JSON 策略文档	629
了解更多信息	630
AmazonKinesisFirehoseReadOnlyAccess	630
使用此策略	630
策略详细信息	630
策略版本	630
JSON 策略文档	631
了解更多信息	631
AmazonKinesisFullAccess	631
使用此策略	631
策略详细信息	631
策略版本	632
JSON 策略文档	632
了解更多信息	632
AmazonKinesisReadOnlyAccess	632
使用此策略	633
策略详细信息	633
策略版本	633
JSON 策略文档	633
了解更多信息	633

AmazonKinesisVideoStreamsFullAccess	634
使用此策略	634
策略详细信息	634
策略版本	634
JSON 策略文档	634
了解更多信息	635
AmazonKinesisVideoStreamsReadOnlyAccess	635
使用此策略	635
策略详细信息	635
策略版本	635
JSON 策略文档	635
了解更多信息	636
AmazonLaunchWizard_Fullaccess	636
使用此策略	636
策略详细信息	636
策略版本	636
JSON 策略文档	637
了解更多信息	651
AmazonLaunchWizardFullAccessV2	651
使用此策略	651
策略详细信息	651
策略版本	651
JSON 策略文档	652
了解更多信息	668
AmazonLexChannelsAccess	668
使用此策略	668
策略详细信息	668
策略版本	669
JSON 策略文档	669
了解更多信息	669
AmazonLexFullAccess	669
使用此策略	670
策略详细信息	670
策略版本	670
JSON 策略文档	670
了解更多信息	675

AmazonLexReadOnly	676
使用此策略	676
策略详细信息	676
策略版本	676
JSON 策略文档	676
了解更多信息	678
AmazonLexReplicationPolicy	678
使用此策略	678
策略详细信息	678
策略版本	678
JSON 策略文档	679
了解更多信息	681
AmazonLexRunBotsOnly	681
使用此策略	681
策略详细信息	681
策略版本	681
JSON 策略文档	682
了解更多信息	682
AmazonLexV2BotPolicy	682
使用此策略	682
策略详细信息	683
策略版本	683
JSON 策略文档	683
了解更多信息	683
AmazonLookoutEquipmentFullAccess	684
使用此策略	684
策略详细信息	684
策略版本	684
JSON 策略文档	684
了解更多信息	685
AmazonLookoutEquipmentReadOnlyAccess	686
使用此策略	686
策略详细信息	686
策略版本	686
JSON 策略文档	686
了解更多信息	687

AmazonLookoutMetricsFullAccess	687
使用此策略	687
策略详细信息	687
策略版本	687
JSON 策略文档	687
了解更多信息	688
AmazonLookoutMetricsReadOnlyAccess	688
使用此策略	688
策略详细信息	689
策略版本	689
JSON 策略文档	689
了解更多信息	690
AmazonLookoutVisionConsoleFullAccess	690
使用此策略	690
策略详细信息	690
策略版本	690
JSON 策略文档	690
了解更多信息	693
AmazonLookoutVisionConsoleReadOnlyAccess	693
使用此策略	693
策略详细信息	693
策略版本	693
JSON 策略文档	694
了解更多信息	695
AmazonLookoutVisionFullAccess	695
使用此策略	695
策略详细信息	695
策略版本	695
JSON 策略文档	696
了解更多信息	696
AmazonLookoutVisionReadOnlyAccess	696
使用此策略	696
策略详细信息	696
策略版本	697
JSON 策略文档	697
了解更多信息	697

AmazonMachineLearningBatchPredictionsAccess	698
使用此策略	698
策略详细信息	698
策略版本	698
JSON 策略文档	698
了解更多信息	699
AmazonMachineLearningCreateOnlyAccess	699
使用此策略	699
策略详细信息	699
策略版本	699
JSON 策略文档	700
了解更多信息	700
AmazonMachineLearningFullAccess	700
使用此策略	700
策略详细信息	700
策略版本	701
JSON 策略文档	701
了解更多信息	701
AmazonMachineLearningManageRealTimeEndpointOnlyAccess	701
使用此策略	702
策略详细信息	702
策略版本	702
JSON 策略文档	702
了解更多信息	702
AmazonMachineLearningReadOnlyAccess	703
使用此策略	703
策略详细信息	703
策略版本	703
JSON 策略文档	703
了解更多信息	704
AmazonMachineLearningRealTimePredictionOnlyAccess	704
使用此策略	704
策略详细信息	704
策略版本	704
JSON 策略文档	705
了解更多信息	705

AmazonMachineLearningRoleforRedshiftDataSourceV3	705
使用此策略	705
策略详细信息	705
策略版本	706
JSON 策略文档	706
了解更多信息	707
AmazonMacieFullAccess	707
使用此策略	707
策略详细信息	707
策略版本	707
JSON 策略文档	707
了解更多信息	708
AmazonMacieHandshakeRole	708
使用此策略	709
策略详细信息	709
策略版本	709
JSON 策略文档	709
了解更多信息	709
AmazonMacieReadOnlyAccess	710
使用此策略	710
策略详细信息	710
策略版本	710
JSON 策略文档	710
了解更多信息	711
AmazonMacieServiceRole	711
使用此策略	711
策略详细信息	711
策略版本	711
JSON 策略文档	712
了解更多信息	712
AmazonMacieServiceRolePolicy	712
使用此策略	712
策略详细信息	712
策略版本	713
JSON 策略文档	713
了解更多信息	714

AmazonManagedBlockchainConsoleFullAccess	714
使用此策略	714
策略详细信息	714
策略版本	715
JSON 策略文档	715
了解更多信息	715
AmazonManagedBlockchainFullAccess	716
使用此策略	716
策略详细信息	716
策略版本	716
JSON 策略文档	716
了解更多信息	717
AmazonManagedBlockchainReadOnlyAccess	717
使用此策略	717
策略详细信息	717
策略版本	717
JSON 策略文档	717
了解更多信息	718
AmazonManagedBlockchainServiceRolePolicy	718
使用此策略	718
策略详细信息	718
策略版本	719
JSON 策略文档	719
了解更多信息	719
AmazonMCSFullAccess	719
使用此策略	720
策略详细信息	720
策略版本	720
JSON 策略文档	720
了解更多信息	721
AmazonMCSReadOnlyAccess	721
使用此策略	722
策略详细信息	722
策略版本	722
JSON 策略文档	722
了解更多信息	723

AmazonMechanicalTurkFullAccess	723
使用此策略	723
策略详细信息	723
策略版本	723
JSON 策略文档	724
了解更多信息	724
AmazonMechanicalTurkReadOnly	724
使用此策略	724
策略详细信息	724
策略版本	725
JSON 策略文档	725
了解更多信息	725
AmazonMemoryDBFullAccess	725
使用此策略	726
策略详细信息	726
策略版本	726
JSON 策略文档	726
了解更多信息	727
AmazonMemoryDBReadOnlyAccess	727
使用此策略	727
策略详细信息	727
策略版本	727
JSON 策略文档	728
了解更多信息	728
AmazonMobileAnalyticsFinancialReportAccess	728
使用此策略	728
策略详细信息	728
策略版本	729
JSON 策略文档	729
了解更多信息	729
AmazonMobileAnalyticsFullAccess	729
使用此策略	730
策略详细信息	730
策略版本	730
JSON 策略文档	730
了解更多信息	730

AmazonMobileAnalyticsNon-financialReportAccess	731
使用此策略	731
策略详细信息	731
策略版本	731
JSON 策略文档	731
了解更多信息	732
AmazonMobileAnalyticsWriteOnlyAccess	732
使用此策略	732
策略详细信息	732
策略版本	732
JSON 策略文档	732
了解更多信息	733
AmazonMonitronFullAccess	733
使用此策略	733
策略详细信息	733
策略版本	733
JSON 策略文档	734
了解更多信息	735
AmazonMQApiFullAccess	736
使用此策略	736
策略详细信息	736
策略版本	736
JSON 策略文档	736
了解更多信息	737
AmazonMQApiReadOnlyAccess	738
使用此策略	738
策略详细信息	738
策略版本	738
JSON 策略文档	738
了解更多信息	739
AmazonMQFullAccess	739
使用此策略	739
策略详细信息	739
策略版本	739
JSON 策略文档	740
了解更多信息	741

AmazonMQReadOnlyAccess	741
使用此策略	741
策略详细信息	741
策略版本	741
JSON 策略文档	742
了解更多信息	742
AmazonMQServiceRolePolicy	742
使用此策略	742
策略详细信息	742
策略版本	743
JSON 策略文档	743
了解更多信息	745
AmazonMSKConnectReadOnlyAccess	745
使用此策略	745
策略详细信息	745
策略版本	745
JSON 策略文档	745
了解更多信息	746
AmazonMSKFullAccess	747
使用此策略	747
策略详细信息	747
策略版本	747
JSON 策略文档	747
了解更多信息	750
AmazonMSKReadOnlyAccess	750
使用此策略	750
策略详细信息	750
策略版本	751
JSON 策略文档	751
了解更多信息	751
AmazonMWAAServiceRolePolicy	752
使用此策略	752
策略详细信息	752
策略版本	752
JSON 策略文档	752
了解更多信息	754

AmazonNimbleStudio-LaunchProfileWorker	755
使用此策略	755
策略详细信息	755
策略版本	755
JSON 策略文档	755
了解更多信息	756
AmazonNimbleStudio-StudioAdmin	756
使用此策略	756
策略详细信息	756
策略版本	757
JSON 策略文档	757
了解更多信息	759
AmazonNimbleStudio-StudioUser	759
使用此策略	759
策略详细信息	759
策略版本	759
JSON 策略文档	759
了解更多信息	761
AmazonOmicsFullAccess	762
使用此策略	762
策略详细信息	762
策略版本	762
JSON 策略文档	762
了解更多信息	763
AmazonOmicsReadOnlyAccess	763
使用此策略	764
策略详细信息	764
策略版本	764
JSON 策略文档	764
了解更多信息	764
AmazonOneEnterpriseFullAccess	765
使用此策略	765
策略详细信息	765
策略版本	765
JSON 策略文档	765
了解更多信息	766

AmazonOneEnterpriseInstallerAccess	766
使用此策略	766
策略详细信息	766
策略版本	766
JSON 策略文档	766
了解更多信息	767
AmazonOneEnterpriseReadOnlyAccess	767
使用此策略	767
策略详细信息	767
策略版本	768
JSON 策略文档	768
了解更多信息	768
AmazonOpenSearchDashboardsServiceRolePolicy	768
使用此策略	769
策略详细信息	769
策略版本	769
JSON 策略文档	769
了解更多信息	770
AmazonOpenSearchDirectQueryGlueCreateAccess	770
使用此策略	770
策略详细信息	770
策略版本	770
JSON 策略文档	770
了解更多信息	771
AmazonOpenSearchIngestionFullAccess	771
使用此策略	771
策略详细信息	771
策略版本	771
JSON 策略文档	772
了解更多信息	773
AmazonOpenSearchIngestionReadOnlyAccess	773
使用此策略	773
策略详细信息	773
策略版本	773
JSON 策略文档	773
了解更多信息	774

AmazonOpenSearchIngestionServiceRolePolicy	774
使用此策略	774
策略详细信息	774
策略版本	775
JSON 策略文档	775
了解更多信息	777
AmazonOpenSearchServerlessServiceRolePolicy	777
使用此策略	777
策略详细信息	777
策略版本	777
JSON 策略文档	777
了解更多信息	778
AmazonOpenSearchServiceCognitoAccess	778
使用此策略	778
策略详细信息	778
策略版本	778
JSON 策略文档	779
了解更多信息	780
AmazonOpenSearchServiceFullAccess	780
使用此策略	780
策略详细信息	780
策略版本	780
JSON 策略文档	780
了解更多信息	781
AmazonOpenSearchServiceReadOnlyAccess	781
使用此策略	781
策略详细信息	781
策略版本	781
JSON 策略文档	782
了解更多信息	782
AmazonOpenSearchServiceRolePolicy	782
使用此策略	782
策略详细信息	782
策略版本	783
JSON 策略文档	783
了解更多信息	787

AmazonPersonalizeFullAccess	788
使用此策略	788
策略详细信息	788
策略版本	788
JSON 策略文档	788
了解更多信息	789
AmazonPollyFullAccess	790
使用此策略	790
策略详细信息	790
策略版本	790
JSON 策略文档	790
了解更多信息	791
AmazonPollyReadOnlyAccess	791
使用此策略	791
策略详细信息	791
策略版本	791
JSON 策略文档	791
了解更多信息	792
AmazonPrometheusConsoleFullAccess	792
使用此策略	792
策略详细信息	792
策略版本	793
JSON 策略文档	793
了解更多信息	794
AmazonPrometheusFullAccess	794
使用此策略	794
策略详细信息	794
策略版本	794
JSON 策略文档	795
了解更多信息	796
AmazonPrometheusQueryAccess	796
使用此策略	796
策略详细信息	796
策略版本	796
JSON 策略文档	796
了解更多信息	797

AmazonPrometheusRemoteWriteAccess	797
使用此策略	797
策略详细信息	797
策略版本	798
JSON 策略文档	798
了解更多信息	798
AmazonPrometheusScraperServiceRolePolicy	798
使用此策略	798
策略详细信息	799
策略版本	799
JSON 策略文档	799
了解更多信息	801
AmazonQFullAccess	801
使用此策略	802
策略详细信息	802
策略版本	802
JSON 策略文档	802
了解更多信息	803
AmazonQLDBConsoleFullAccess	803
使用此策略	803
策略详细信息	803
策略版本	803
JSON 策略文档	803
了解更多信息	805
AmazonQLDBFullAccess	805
使用此策略	805
策略详细信息	806
策略版本	806
JSON 策略文档	806
了解更多信息	807
AmazonQLDBReadOnly	807
使用此策略	808
策略详细信息	808
策略版本	808
JSON 策略文档	808
了解更多信息	809

AmazonRDSBetaServiceRolePolicy	809
使用此策略	809
策略详细信息	809
策略版本	809
JSON 策略文档	810
了解更多信息	813
AmazonRDSCustomInstanceProfileRolePolicy	813
使用此策略	813
策略详细信息	813
策略版本	813
JSON 策略文档	813
了解更多信息	821
AmazonRDSCustomPreviewServiceRolePolicy	821
使用此策略	821
策略详细信息	821
策略版本	821
JSON 策略文档	821
了解更多信息	837
AmazonRDSCustomServiceRolePolicy	837
使用此策略	837
策略详细信息	837
策略版本	838
JSON 策略文档	838
了解更多信息	855
AmazonRDSDataFullAccess	855
使用此策略	855
策略详细信息	855
策略版本	856
JSON 策略文档	856
了解更多信息	857
AmazonRDSDirectoryServiceAccess	857
使用此策略	857
策略详细信息	857
策略版本	858
JSON 策略文档	858
了解更多信息	858

AmazonRDSEnhancedMonitoringRole	858
使用此策略	859
策略详细信息	859
策略版本	859
JSON 策略文档	859
了解更多信息	860
AmazonRDSFullAccess	860
使用此策略	860
策略详细信息	860
策略版本	860
JSON 策略文档	861
了解更多信息	863
AmazonRDSPerformanceInsightsFullAccess	863
使用此策略	863
策略详细信息	863
策略版本	863
JSON 策略文档	863
了解更多信息	865
AmazonRDSPerformanceInsightsReadOnly	865
使用此策略	865
策略详细信息	865
策略版本	866
JSON 策略文档	866
了解更多信息	867
AmazonRDSPreviewServiceRolePolicy	868
使用此策略	868
策略详细信息	868
策略版本	868
JSON 策略文档	868
了解更多信息	871
AmazonRDSReadOnlyAccess	872
使用此策略	872
策略详细信息	872
策略版本	872
JSON 策略文档	872
了解更多信息	873

AmazonRDSServiceRolePolicy	874
使用此策略	874
策略详细信息	874
策略版本	874
JSON 策略文档	874
了解更多信息	878
AmazonRedshiftAllCommandsFullAccess	878
使用此策略	879
策略详细信息	879
策略版本	879
JSON 策略文档	879
了解更多信息	884
AmazonRedshiftDataFullAccess	884
使用此策略	885
策略详细信息	885
策略版本	885
JSON 策略文档	885
了解更多信息	887
AmazonRedshiftFullAccess	887
使用此策略	887
策略详细信息	887
策略版本	888
JSON 策略文档	888
了解更多信息	890
AmazonRedshiftQueryEditor	890
使用此策略	890
策略详细信息	890
策略版本	891
JSON 策略文档	891
了解更多信息	893
AmazonRedshiftQueryEditorV2FullAccess	893
使用此策略	893
策略详细信息	893
策略版本	893
JSON 策略文档	893
了解更多信息	895

AmazonRedshiftQueryEditorV2NoSharing	895
使用此策略	895
策略详细信息	895
策略版本	896
JSON 策略文档	896
了解更多信息	899
AmazonRedshiftQueryEditorV2ReadSharing	900
使用此策略	900
策略详细信息	900
策略版本	900
JSON 策略文档	900
了解更多信息	905
AmazonRedshiftQueryEditorV2ReadWriteSharing	905
使用此策略	906
策略详细信息	906
策略版本	906
JSON 策略文档	906
了解更多信息	911
AmazonRedshiftReadOnlyAccess	911
使用此策略	911
策略详细信息	911
策略版本	912
JSON 策略文档	912
了解更多信息	913
AmazonRedshiftServiceLinkedRolePolicy	913
使用此策略	913
策略详细信息	913
策略版本	913
JSON 策略文档	913
了解更多信息	919
AmazonRekognitionCustomLabelsFullAccess	919
使用此策略	919
策略详细信息	919
策略版本	919
JSON 策略文档	920
了解更多信息	921

AmazonRekognitionFullAccess	921
使用此策略	921
策略详细信息	921
策略版本	921
JSON 策略文档	922
了解更多信息	922
AmazonRekognitionReadOnlyAccess	922
使用此策略	922
策略详细信息	922
策略版本	923
JSON 策略文档	923
了解更多信息	924
AmazonRekognitionServiceRole	924
使用此策略	924
策略详细信息	924
策略版本	925
JSON 策略文档	925
了解更多信息	926
AmazonRoute53AutoNamingFullAccess	926
使用此策略	926
策略详细信息	926
策略版本	926
JSON 策略文档	926
了解更多信息	927
AmazonRoute53AutoNamingReadOnlyAccess	927
使用此策略	927
策略详细信息	928
策略版本	928
JSON 策略文档	928
了解更多信息	928
AmazonRoute53AutoNamingRegistrantAccess	929
使用此策略	929
策略详细信息	929
策略版本	929
JSON 策略文档	929
了解更多信息	930

AmazonRoute53DomainsFullAccess	930
使用此策略	930
策略详细信息	930
策略版本	931
JSON 策略文档	931
了解更多信息	931
AmazonRoute53DomainsReadOnlyAccess	931
使用此策略	932
策略详细信息	932
策略版本	932
JSON 策略文档	932
了解更多信息	932
AmazonRoute53FullAccess	933
使用此策略	933
策略详细信息	933
策略版本	933
JSON 策略文档	933
了解更多信息	934
AmazonRoute53ProfilesFullAccess	934
使用此策略	934
策略详细信息	935
策略版本	935
JSON 策略文档	935
了解更多信息	936
AmazonRoute53ProfilesReadOnlyAccess	936
使用此策略	936
策略详细信息	936
策略版本	937
JSON 策略文档	937
了解更多信息	937
AmazonRoute53ReadOnlyAccess	938
使用此策略	938
策略详细信息	938
策略版本	938
JSON 策略文档	938
了解更多信息	939

AmazonRoute53RecoveryClusterFullAccess	939
使用此策略	939
策略详细信息	939
策略版本	939
JSON 策略文档	939
了解更多信息	940
AmazonRoute53RecoveryClusterReadOnlyAccess	940
使用此策略	940
策略详细信息	940
策略版本	940
JSON 策略文档	941
了解更多信息	941
AmazonRoute53RecoveryControlConfigFullAccess	941
使用此策略	941
策略详细信息	941
策略版本	942
JSON 策略文档	942
了解更多信息	942
AmazonRoute53RecoveryControlConfigReadOnlyAccess	942
使用此策略	943
策略详细信息	943
策略版本	943
JSON 策略文档	943
了解更多信息	944
AmazonRoute53RecoveryReadinessFullAccess	944
使用此策略	944
策略详细信息	944
策略版本	944
JSON 策略文档	945
了解更多信息	945
AmazonRoute53RecoveryReadinessReadOnlyAccess	945
使用此策略	945
策略详细信息	945
策略版本	946
JSON 策略文档	946
了解更多信息	947

AmazonRoute53ResolverFullAccess	947
使用此策略	947
策略详细信息	947
策略版本	947
JSON 策略文档	947
了解更多信息	948
AmazonRoute53ResolverReadOnlyAccess	948
使用此策略	948
策略详细信息	948
策略版本	949
JSON 策略文档	949
了解更多信息	949
AmazonS3FullAccess	950
使用此策略	950
策略详细信息	950
策略版本	950
JSON 策略文档	950
了解更多信息	951
AmazonS3ObjectLambdaExecutionRolePolicy	951
使用此策略	951
策略详细信息	951
策略版本	951
JSON 策略文档	951
了解更多信息	952
AmazonS3OutpostsFullAccess	952
使用此策略	952
策略详细信息	952
策略版本	953
JSON 策略文档	953
了解更多信息	954
AmazonS3OutpostsReadOnlyAccess	954
使用此策略	954
策略详细信息	954
策略版本	954
JSON 策略文档	955
了解更多信息	956

AmazonS3ReadOnlyAccess	956
使用此策略	956
策略详细信息	956
策略版本	956
JSON 策略文档	956
了解更多信息	957
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	957
使用此策略	957
策略详细信息	957
策略版本	958
JSON 策略文档	958
了解更多信息	968
AmazonSageMakerCanvasAIServiceAccess	968
使用此策略	968
策略详细信息	968
策略版本	968
JSON 策略文档	969
了解更多信息	972
AmazonSageMakerCanvasBedrockAccess	972
使用此策略	972
策略详细信息	972
策略版本	972
JSON 策略文档	972
了解更多信息	973
AmazonSageMakerCanvasDataPrepFullAccess	973
使用此策略	974
策略详细信息	974
策略版本	974
JSON 策略文档	974
了解更多信息	981
AmazonSageMakerCanvasDirectDeployAccess	981
使用此策略	981
策略详细信息	981
策略版本	982
JSON 策略文档	982
了解更多信息	983

AmazonSageMakerCanvasForecastAccess	983
使用此策略	983
策略详细信息	983
策略版本	983
JSON 策略文档	983
了解更多信息	984
AmazonSageMakerCanvasFullAccess	984
使用此策略	985
策略详细信息	985
策略版本	985
JSON 策略文档	985
了解更多信息	993
AmazonSageMakerClusterInstanceRolePolicy	993
使用此策略	993
策略详细信息	993
策略版本	994
JSON 策略文档	994
了解更多信息	995
AmazonSageMakerCoreServiceRolePolicy	996
使用此策略	996
策略详细信息	996
策略版本	996
JSON 策略文档	996
了解更多信息	997
AmazonSageMakerEdgeDeviceFleetPolicy	997
使用此策略	997
策略详细信息	998
策略版本	998
JSON 策略文档	998
了解更多信息	1000
AmazonSageMakerFeatureStoreAccess	1000
使用此策略	1000
策略详细信息	1000
策略版本	1000
JSON 策略文档	1001
了解更多信息	1002

AmazonSageMakerFullAccess	1002
使用此策略	1002
策略详细信息	1002
策略版本	1002
JSON 策略文档	1002
了解更多信息	1018
AmazonSageMakerGeospatialExecutionRole	1019
使用此策略	1019
策略详细信息	1019
策略版本	1019
JSON 策略文档	1019
了解更多信息	1020
AmazonSageMakerGeospatialFullAccess	1020
使用此策略	1020
策略详细信息	1020
策略版本	1021
JSON 策略文档	1021
了解更多信息	1021
AmazonSageMakerGroundTruthExecution	1022
使用此策略	1022
策略详细信息	1022
策略版本	1022
JSON 策略文档	1022
了解更多信息	1026
AmazonSageMakerMechanicalTurkAccess	1026
使用此策略	1026
策略详细信息	1026
策略版本	1026
JSON 策略文档	1027
了解更多信息	1027
AmazonSageMakerModelGovernanceUseAccess	1027
使用此策略	1027
策略详细信息	1027
策略版本	1028
JSON 策略文档	1028
了解更多信息	1030

AmazonSageMakerModelRegistryFullAccess	1030
使用此策略	1030
策略详细信息	1030
策略版本	1030
JSON 策略文档	1030
了解更多信息	1034
AmazonSageMakerNotebooksServiceRolePolicy	1034
使用此策略	1034
策略详细信息	1035
策略版本	1035
JSON 策略文档	1035
了解更多信息	1039
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1039
使用此策略	1039
策略详细信息	1039
策略版本	1040
JSON 策略文档	1040
了解更多信息	1041
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1041
使用此策略	1041
策略详细信息	1041
策略版本	1041
JSON 策略文档	1042
了解更多信息	1045
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1045
使用此策略	1045
策略详细信息	1045
策略版本	1046
JSON 策略文档	1046
了解更多信息	1046
AmazonSageMakerPipelinesIntegrations	1047
使用此策略	1047
策略详细信息	1047
策略版本	1047
JSON 策略文档	1047
了解更多信息	1049

AmazonSageMakerReadOnly	1049
使用此策略	1049
策略详细信息	1050
策略版本	1050
JSON 策略文档	1050
了解更多信息	1051
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1051
使用此策略	1051
策略详细信息	1052
策略版本	1052
JSON 策略文档	1052
了解更多信息	1053
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1053
使用此策略	1053
策略详细信息	1053
策略版本	1054
JSON 策略文档	1054
了解更多信息	1060
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1061
使用此策略	1061
策略详细信息	1061
策略版本	1061
JSON 策略文档	1061
了解更多信息	1071
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1072
使用此策略	1072
策略详细信息	1072
策略版本	1072
JSON 策略文档	1072
了解更多信息	1075
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1075
使用此策略	1076
策略详细信息	1076
策略版本	1076
JSON 策略文档	1076
了解更多信息	1076

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1077
使用此策略	1077
策略详细信息	1077
策略版本	1077
JSON 策略文档	1077
了解更多信息	1078
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1078
使用此策略	1078
策略详细信息	1078
策略版本	1079
JSON 策略文档	1079
了解更多信息	1081
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1081
使用此策略	1081
策略详细信息	1081
策略版本	1082
JSON 策略文档	1082
了解更多信息	1092
AmazonSecurityLakeAdministrator	1092
使用此策略	1092
策略详细信息	1092
策略版本	1092
JSON 策略文档	1093
了解更多信息	1104
AmazonSecurityLakeMetastoreManager	1104
使用此策略	1104
策略详细信息	1104
策略版本	1104
JSON 策略文档	1105
了解更多信息	1107
AmazonSecurityLakePermissionsBoundary	1107
使用此策略	1107
策略详细信息	1107
策略版本	1108
JSON 策略文档	1108
了解更多信息	1111

AmazonSESEFullAccess	1111
使用此策略	1111
策略详细信息	1111
策略版本	1112
JSON 策略文档	1112
了解更多信息	1112
AmazonSESReadOnlyAccess	1112
使用此策略	1112
策略详细信息	1113
策略版本	1113
JSON 策略文档	1113
了解更多信息	1113
AmazonSESServiceRolePolicy	1114
使用此策略	1114
策略详细信息	1114
策略版本	1114
JSON 策略文档	1114
了解更多信息	1115
AmazonSNSFullAccess	1115
使用此策略	1115
策略详细信息	1115
策略版本	1115
JSON 策略文档	1116
了解更多信息	1116
AmazonSNSReadOnlyAccess	1116
使用此策略	1116
策略详细信息	1116
策略版本	1117
JSON 策略文档	1117
了解更多信息	1117
AmazonSNSRole	1117
使用此策略	1117
策略详细信息	1118
策略版本	1118
JSON 策略文档	1118
了解更多信息	1118

AmazonSQSFullAccess	1119
使用此策略	1119
策略详细信息	1119
策略版本	1119
JSON 策略文档	1119
了解更多信息	1120
AmazonSQSReadOnlyAccess	1120
使用此策略	1120
策略详细信息	1120
策略版本	1120
JSON 策略文档	1120
了解更多信息	1121
AmazonSSMAutomationApproverAccess	1121
使用此策略	1121
策略详细信息	1121
策略版本	1122
JSON 策略文档	1122
了解更多信息	1122
AmazonSSMAutomationRole	1122
使用此策略	1123
策略详细信息	1123
策略版本	1123
JSON 策略文档	1123
了解更多信息	1124
AmazonSSMDirectoryServiceAccess	1125
使用此策略	1125
策略详细信息	1125
策略版本	1125
JSON 策略文档	1125
了解更多信息	1126
AmazonSSMFullAccess	1126
使用此策略	1126
策略详细信息	1126
策略版本	1126
JSON 策略文档	1127
了解更多信息	1128

AmazonSSMMaintenanceWindowRole	1128
使用此策略	1128
策略详细信息	1128
策略版本	1128
JSON 策略文档	1129
了解更多信息	1130
AmazonSSMManagedEC2InstanceDefaultPolicy	1130
使用此策略	1130
策略详细信息	1130
策略版本	1131
JSON 策略文档	1131
了解更多信息	1132
AmazonSSMManagedInstanceCore	1132
使用此策略	1132
策略详细信息	1132
策略版本	1133
JSON 策略文档	1133
了解更多信息	1134
AmazonSSMPatchAssociation	1134
使用此策略	1134
策略详细信息	1134
策略版本	1135
JSON 策略文档	1135
了解更多信息	1135
AmazonSSMReadOnlyAccess	1136
使用此策略	1136
策略详细信息	1136
策略版本	1136
JSON 策略文档	1136
了解更多信息	1137
AmazonSSMServiceRolePolicy	1137
使用此策略	1137
策略详细信息	1137
策略版本	1137
JSON 策略文档	1138
了解更多信息	1143

AmazonSumerianFullAccess	1143
使用此策略	1143
策略详细信息	1143
策略版本	1143
JSON 策略文档	1143
了解更多信息	1144
AmazonTextractFullAccess	1144
使用此策略	1144
策略详细信息	1144
策略版本	1144
JSON 策略文档	1145
了解更多信息	1145
AmazonTextractServiceRole	1145
使用此策略	1145
策略详细信息	1145
策略版本	1146
JSON 策略文档	1146
了解更多信息	1146
AmazonTimestreamConsoleFullAccess	1146
使用此策略	1147
策略详细信息	1147
策略版本	1147
JSON 策略文档	1147
了解更多信息	1149
AmazonTimestreamFullAccess	1149
使用此策略	1149
策略详细信息	1149
策略版本	1149
JSON 策略文档	1150
了解更多信息	1151
AmazonTimestreamInfluxDBFullAccess	1151
使用此策略	1151
策略详细信息	1151
策略版本	1151
JSON 策略文档	1152
了解更多信息	1153

AmazonTimestreamInfluxDBServiceRolePolicy	1154
使用此策略	1154
策略详细信息	1154
策略版本	1154
JSON 策略文档	1154
了解更多信息	1157
AmazonTimestreamReadOnlyAccess	1157
使用此策略	1157
策略详细信息	1157
策略版本	1157
JSON 策略文档	1158
了解更多信息	1158
AmazonTranscribeFullAccess	1158
使用此策略	1159
策略详细信息	1159
策略版本	1159
JSON 策略文档	1159
了解更多信息	1160
AmazonTranscribeReadOnlyAccess	1160
使用此策略	1160
策略详细信息	1160
策略版本	1160
JSON 策略文档	1160
了解更多信息	1161
AmazonVPCCrossAccountNetworkInterfaceOperations	1161
使用此策略	1161
策略详细信息	1161
策略版本	1162
JSON 策略文档	1162
了解更多信息	1163
AmazonVPCFullAccess	1163
使用此策略	1163
策略详细信息	1164
策略版本	1164
JSON 策略文档	1164
了解更多信息	1168

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1168
使用此策略	1168
策略详细信息	1168
策略版本	1168
JSON 策略文档	1169
了解更多信息	1172
AmazonVPCReachabilityAnalyzerFullAccessPolicy	1172
使用此策略	1172
策略详细信息	1172
策略版本	1173
JSON 策略文档	1173
了解更多信息	1176
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1176
使用此策略	1176
策略详细信息	1176
策略版本	1177
JSON 策略文档	1177
了解更多信息	1177
AmazonVPCReadOnlyAccess	1177
使用此策略	1177
策略详细信息	1178
策略版本	1178
JSON 策略文档	1178
了解更多信息	1179
AmazonWorkDocsFullAccess	1179
使用此策略	1180
策略详细信息	1180
策略版本	1180
JSON 策略文档	1180
了解更多信息	1180
AmazonWorkDocsReadOnlyAccess	1181
使用此策略	1181
策略详细信息	1181
策略版本	1181
JSON 策略文档	1181
了解更多信息	1182

AmazonWorkMailEventsServiceRolePolicy	1182
使用此策略	1182
策略详细信息	1182
策略版本	1182
JSON 策略文档	1183
了解更多信息	1183
AmazonWorkMailFullAccess	1183
使用此策略	1183
策略详细信息	1183
策略版本	1184
JSON 策略文档	1184
了解更多信息	1186
AmazonWorkMailMessageFlowFullAccess	1186
使用此策略	1186
策略详细信息	1186
策略版本	1186
JSON 策略文档	1187
了解更多信息	1187
AmazonWorkMailMessageFlowReadOnlyAccess	1187
使用此策略	1187
策略详细信息	1187
策略版本	1188
JSON 策略文档	1188
了解更多信息	1188
AmazonWorkMailReadOnlyAccess	1188
使用此策略	1188
策略详细信息	1189
策略版本	1189
JSON 策略文档	1189
了解更多信息	1190
AmazonWorkSpacesAdmin	1190
使用此策略	1190
策略详细信息	1190
策略版本	1190
JSON 策略文档	1190
了解更多信息	1191

AmazonWorkSpacesApplicationManagerAdminAccess	1191
使用此策略	1192
策略详细信息	1192
策略版本	1192
JSON 策略文档	1192
了解更多信息	1192
AmazonWorkspacesPCAAccess	1193
使用此策略	1193
策略详细信息	1193
策略版本	1193
JSON 策略文档	1193
了解更多信息	1194
AmazonWorkSpacesSelfServiceAccess	1194
使用此策略	1194
策略详细信息	1194
策略版本	1194
JSON 策略文档	1195
了解更多信息	1195
AmazonWorkSpacesServiceAccess	1195
使用此策略	1195
策略详细信息	1195
策略版本	1196
JSON 策略文档	1196
了解更多信息	1196
AmazonWorkSpacesWebReadOnly	1196
使用此策略	1197
策略详细信息	1197
策略版本	1197
JSON 策略文档	1197
了解更多信息	1198
AmazonWorkSpacesWebServiceRolePolicy	1198
使用此策略	1198
策略详细信息	1198
策略版本	1199
JSON 策略文档	1199
了解更多信息	1201

AmazonZocaloFullAccess	1201
使用此策略	1201
策略详细信息	1202
策略版本	1202
JSON 策略文档	1202
了解更多信息	1203
AmazonZocaloReadOnlyAccess	1203
使用此策略	1203
策略详细信息	1203
策略版本	1203
JSON 策略文档	1203
了解更多信息	1204
AmplifyBackendDeployFullAccess	1204
使用此策略	1204
策略详细信息	1204
策略版本	1205
JSON 策略文档	1205
了解更多信息	1209
APIGatewayServiceRolePolicy	1209
使用此策略	1209
策略详细信息	1209
策略版本	1209
JSON 策略文档	1209
了解更多信息	1212
AppIntegrationsServiceLinkedRolePolicy	1212
使用此策略	1212
策略详细信息	1212
策略版本	1212
JSON 策略文档	1212
了解更多信息	1214
ApplicationAutoScalingForAmazonAppStreamAccess	1214
使用此策略	1214
策略详细信息	1214
策略版本	1215
JSON 策略文档	1215
了解更多信息	1215

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1216
使用此策略	1216
策略详细信息	1216
策略版本	1216
JSON 策略文档	1216
了解更多信息	1218
AppRunnerNetworkingServiceRolePolicy	1218
使用此策略	1219
策略详细信息	1219
策略版本	1219
JSON 策略文档	1219
了解更多信息	1220
AppRunnerServiceRolePolicy	1220
使用此策略	1221
策略详细信息	1221
策略版本	1221
JSON 策略文档	1221
了解更多信息	1222
AutoScalingConsoleFullAccess	1222
使用此策略	1222
策略详细信息	1222
策略版本	1223
JSON 策略文档	1223
了解更多信息	1224
AutoScalingConsoleReadOnlyAccess	1225
使用此策略	1225
策略详细信息	1225
策略版本	1225
JSON 策略文档	1225
了解更多信息	1226
AutoScalingFullAccess	1227
使用此策略	1227
策略详细信息	1227
策略版本	1227
JSON 策略文档	1227
了解更多信息	1228

AutoScalingNotificationAccessRole	1229
使用此策略	1229
策略详细信息	1229
策略版本	1229
JSON 策略文档	1229
了解更多信息	1230
AutoScalingReadOnlyAccess	1230
使用此策略	1230
策略详细信息	1230
策略版本	1230
JSON 策略文档	1231
了解更多信息	1231
AutoScalingServiceRolePolicy	1231
使用此策略	1231
策略详细信息	1231
策略版本	1232
JSON 策略文档	1232
了解更多信息	1235
AWS_ConfigRole	1235
使用此策略	1235
策略详细信息	1235
策略版本	1235
JSON 策略文档	1235
了解更多信息	1266
AWSAccountActivityAccess	1266
使用此策略	1266
策略详细信息	1266
策略版本	1267
JSON 策略文档	1267
了解更多信息	1268
AWSAccountManagementFullAccess	1268
使用此策略	1268
策略详细信息	1268
策略版本	1268
JSON 策略文档	1268
了解更多信息	1269

AWSAccountManagementReadOnlyAccess	1269
使用此策略	1269
策略详细信息	1269
策略版本	1269
JSON 策略文档	1270
了解更多信息	1270
AWSAccountUsageReportAccess	1270
使用此策略	1270
策略详细信息	1270
策略版本	1271
JSON 策略文档	1271
了解更多信息	1271
AWSAgentlessDiscoveryService	1271
使用此策略	1272
策略详细信息	1272
策略版本	1272
JSON 策略文档	1272
了解更多信息	1274
AWSAppFabricFullAccess	1274
使用此策略	1274
策略详细信息	1274
策略版本	1275
JSON 策略文档	1275
了解更多信息	1276
AWSAppFabricReadOnlyAccess	1276
使用此策略	1276
策略详细信息	1276
策略版本	1277
JSON 策略文档	1277
了解更多信息	1277
AWSAppFabricServiceRolePolicy	1278
使用此策略	1278
策略详细信息	1278
策略版本	1278
JSON 策略文档	1278
了解更多信息	1279

AWSApplicationAutoscalingAppStreamFleetPolicy	1279
使用此策略	1280
策略详细信息	1280
策略版本	1280
JSON 策略文档	1280
了解更多信息	1281
AWSApplicationAutoscalingCassandraTablePolicy	1281
使用此策略	1281
策略详细信息	1281
策略版本	1281
JSON 策略文档	1281
了解更多信息	1282
AWSApplicationAutoscalingComprehendEndpointPolicy	1282
使用此策略	1282
策略详细信息	1282
策略版本	1283
JSON 策略文档	1283
了解更多信息	1283
AWSApplicationAutoScalingCustomResourcePolicy	1283
使用此策略	1284
策略详细信息	1284
策略版本	1284
JSON 策略文档	1284
了解更多信息	1285
AWSApplicationAutoscalingDynamoDBTablePolicy	1285
使用此策略	1285
策略详细信息	1285
策略版本	1285
JSON 策略文档	1285
了解更多信息	1286
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1286
使用此策略	1286
策略详细信息	1286
策略版本	1286
JSON 策略文档	1287
了解更多信息	1287

AWSApplicationAutoscalingECSServicePolicy	1287
使用此策略	1287
策略详细信息	1288
策略版本	1288
JSON 策略文档	1288
了解更多信息	1288
AWSApplicationAutoscalingElastiCacheRGPolicy	1289
使用此策略	1289
策略详细信息	1289
策略版本	1289
JSON 策略文档	1289
了解更多信息	1290
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1290
使用此策略	1290
策略详细信息	1290
策略版本	1291
JSON 策略文档	1291
了解更多信息	1291
AWSApplicationAutoscalingKafkaClusterPolicy	1291
使用此策略	1292
策略详细信息	1292
策略版本	1292
JSON 策略文档	1292
了解更多信息	1293
AWSApplicationAutoscalingLambdaConcurrencyPolicy	1293
使用此策略	1293
策略详细信息	1293
策略版本	1293
JSON 策略文档	1293
了解更多信息	1294
AWSApplicationAutoscalingNeptuneClusterPolicy	1294
使用此策略	1294
策略详细信息	1294
策略版本	1295
JSON 策略文档	1295
了解更多信息	1296

AWSApplicationAutoscalingRDSClusterPolicy	1296
使用此策略	1297
策略详细信息	1297
策略版本	1297
JSON 策略文档	1297
了解更多信息	1298
AWSApplicationAutoscalingSageMakerEndpointPolicy	1298
使用此策略	1298
策略详细信息	1298
策略版本	1299
JSON 策略文档	1299
了解更多信息	1300
AWSApplicationDiscoveryAgentAccess	1300
使用此策略	1300
策略详细信息	1300
策略版本	1300
JSON 策略文档	1300
了解更多信息	1301
AWSApplicationDiscoveryAgentlessCollectorAccess	1301
使用此策略	1301
策略详细信息	1301
策略版本	1302
JSON 策略文档	1302
了解更多信息	1303
AWSApplicationDiscoveryServiceFullAccess	1303
使用此策略	1303
策略详细信息	1303
策略版本	1303
JSON 策略文档	1304
了解更多信息	1305
AWSApplicationMigrationAgentInstallationPolicy	1305
使用此策略	1305
策略详细信息	1305
策略版本	1306
JSON 策略文档	1306
了解更多信息	1307

AWSApplicationMigrationAgentPolicy	1307
使用此策略	1307
策略详细信息	1307
策略版本	1307
JSON 策略文档	1308
了解更多信息	1308
AWSApplicationMigrationAgentPolicy_v2	1309
使用此策略	1309
策略详细信息	1309
策略版本	1309
JSON 策略文档	1309
了解更多信息	1310
AWSApplicationMigrationConversionServerPolicy	1310
使用此策略	1310
策略详细信息	1311
策略版本	1311
JSON 策略文档	1311
了解更多信息	1311
AWSApplicationMigrationEC2Access	1312
使用此策略	1312
策略详细信息	1312
策略版本	1312
JSON 策略文档	1312
了解更多信息	1320
AWSApplicationMigrationFullAccess	1320
使用此策略	1320
策略详细信息	1320
策略版本	1321
JSON 策略文档	1321
了解更多信息	1327
AWSApplicationMigrationMGHAccess	1327
使用此策略	1327
策略详细信息	1327
策略版本	1327
JSON 策略文档	1328
了解更多信息	1328

AWSApplicationMigrationReadOnlyAccess	1328
使用此策略	1329
策略详细信息	1329
策略版本	1329
JSON 策略文档	1329
了解更多信息	1330
AWSApplicationMigrationReplicationServerPolicy	1330
使用此策略	1331
策略详细信息	1331
策略版本	1331
JSON 策略文档	1331
了解更多信息	1333
AWSApplicationMigrationServiceEc2InstancePolicy	1333
使用此策略	1333
策略详细信息	1333
策略版本	1334
JSON 策略文档	1334
了解更多信息	1335
AWSApplicationMigrationServiceRolePolicy	1335
使用此策略	1335
策略详细信息	1335
策略版本	1335
JSON 策略文档	1336
了解更多信息	1343
AWSApplicationMigrationSSMAccess	1343
使用此策略	1343
策略详细信息	1343
策略版本	1343
JSON 策略文档	1343
了解更多信息	1345
AWSApplicationMigrationVCenterClientPolicy	1346
使用此策略	1346
策略详细信息	1346
策略版本	1346
JSON 策略文档	1346
了解更多信息	1347

AWSAppMeshEnvoyAccess	1347
使用此策略	1347
策略详细信息	1347
策略版本	1348
JSON 策略文档	1348
了解更多信息	1348
AWSAppMeshFullAccess	1348
使用此策略	1349
策略详细信息	1349
策略版本	1349
JSON 策略文档	1349
了解更多信息	1350
AWSAppMeshPreviewEnvoyAccess	1351
使用此策略	1351
策略详细信息	1351
策略版本	1351
JSON 策略文档	1351
了解更多信息	1352
AWSAppMeshPreviewServiceRolePolicy	1352
使用此策略	1352
策略详细信息	1352
策略版本	1352
JSON 策略文档	1352
了解更多信息	1353
AWSAppMeshReadOnly	1353
使用此策略	1353
策略详细信息	1353
策略版本	1354
JSON 策略文档	1354
了解更多信息	1355
AWSAppMeshServiceRolePolicy	1355
使用此策略	1355
策略详细信息	1355
策略版本	1355
JSON 策略文档	1356
了解更多信息	1356

AWSAppRunnerFullAccess	1356
使用此策略	1357
策略详细信息	1357
策略版本	1357
JSON 策略文档	1357
了解更多信息	1358
AWSAppRunnerReadOnlyAccess	1358
使用此策略	1358
策略详细信息	1358
策略版本	1359
JSON 策略文档	1359
了解更多信息	1359
AWSAppRunnerServicePolicyForECRAccess	1359
使用此策略	1359
策略详细信息	1360
策略版本	1360
JSON 策略文档	1360
了解更多信息	1360
AWSAppSyncAdministrator	1361
使用此策略	1361
策略详细信息	1361
策略版本	1361
JSON 策略文档	1361
了解更多信息	1362
AWSAppSyncInvokeFullAccess	1363
使用此策略	1363
策略详细信息	1363
策略版本	1363
JSON 策略文档	1363
了解更多信息	1364
AWSAppSyncPushToCloudWatchLogs	1364
使用此策略	1364
策略详细信息	1364
策略版本	1364
JSON 策略文档	1364
了解更多信息	1365

AWSAppSyncSchemaAuthor	1365
使用此策略	1365
策略详细信息	1365
策略版本	1366
JSON 策略文档	1366
了解更多信息	1367
AWSAppSyncServiceRolePolicy	1367
使用此策略	1367
策略详细信息	1367
策略版本	1367
JSON 策略文档	1368
了解更多信息	1368
AWSArtifactAccountSync	1368
使用此策略	1368
策略详细信息	1368
策略版本	1369
JSON 策略文档	1369
了解更多信息	1369
AWSArtifactReportsReadOnlyAccess	1369
使用此策略	1370
策略详细信息	1370
策略版本	1370
JSON 策略文档	1370
了解更多信息	1371
AWSArtifactServiceRolePolicy	1371
使用此策略	1371
策略详细信息	1371
策略版本	1371
JSON 策略文档	1371
了解更多信息	1372
AWSAuditManagerAdministratorAccess	1372
使用此策略	1372
策略详细信息	1372
策略版本	1372
JSON 策略文档	1373
了解更多信息	1377

AWSAuditManagerServiceRolePolicy	1377
使用此策略	1377
策略详细信息	1377
策略版本	1377
JSON 策略文档	1377
了解更多信息	1384
AWSAutoScalingPlansEC2AutoScalingPolicy	1384
使用此策略	1384
策略详细信息	1385
策略版本	1385
JSON 策略文档	1385
了解更多信息	1385
AWSBackupAuditAccess	1386
使用此策略	1386
策略详细信息	1386
策略版本	1386
JSON 策略文档	1386
了解更多信息	1387
AWSBackupDataTransferAccess	1388
使用此策略	1388
策略详细信息	1388
策略版本	1388
JSON 策略文档	1388
了解更多信息	1389
AWSBackupFullAccess	1389
使用此策略	1389
策略详细信息	1389
策略版本	1390
JSON 策略文档	1390
了解更多信息	1399
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	1400
使用此策略	1400
策略详细信息	1400
策略版本	1400
JSON 策略文档	1400
了解更多信息	1401

AWSBackupOperatorAccess	1401
使用此策略	1401
策略详细信息	1401
策略版本	1402
JSON 策略文档	1402
了解更多信息	1409
AWSBackupOrganizationAdminAccess	1409
使用此策略	1409
策略详细信息	1409
策略版本	1409
JSON 策略文档	1409
了解更多信息	1411
AWSBackupRestoreAccessForSAPHANA	1411
使用此策略	1412
策略详细信息	1412
策略版本	1412
JSON 策略文档	1412
了解更多信息	1413
AWSBackupServiceLinkedRolePolicyForBackup	1413
使用此策略	1413
策略详细信息	1413
策略版本	1414
JSON 策略文档	1414
了解更多信息	1422
AWSBackupServiceLinkedRolePolicyForBackupTest	1422
使用此策略	1422
策略详细信息	1422
策略版本	1422
JSON 策略文档	1423
了解更多信息	1423
AWSBackupServiceRolePolicyForBackup	1423
使用此策略	1424
策略详细信息	1424
策略版本	1424
JSON 策略文档	1424
了解更多信息	1435

AWSBackupServiceRolePolicyForRestores	1435
使用此策略	1435
策略详细信息	1435
策略版本	1436
JSON 策略文档	1436
了解更多信息	1446
AWSBackupServiceRolePolicyForS3Backup	1446
使用此策略	1446
策略详细信息	1446
策略版本	1446
JSON 策略文档	1446
了解更多信息	1449
AWSBackupServiceRolePolicyForS3Restore	1449
使用此策略	1449
策略详细信息	1449
策略版本	1449
JSON 策略文档	1450
了解更多信息	1451
AWSBatchFullAccess	1451
使用此策略	1451
策略详细信息	1451
策略版本	1452
JSON 策略文档	1452
了解更多信息	1453
AWSBatchServiceEventTargetRole	1453
使用此策略	1454
策略详细信息	1454
策略版本	1454
JSON 策略文档	1454
了解更多信息	1454
AWSBatchServiceRole	1455
使用此策略	1455
策略详细信息	1455
策略版本	1455
JSON 策略文档	1455
了解更多信息	1458

AWSBCMDDataExportsServiceRolePolicy	1459
使用此策略	1459
策略详细信息	1459
策略版本	1459
JSON 策略文档	1459
了解更多信息	1460
AWSBillingConductorFullAccess	1460
使用此策略	1460
策略详细信息	1460
策略版本	1460
JSON 策略文档	1460
了解更多信息	1461
AWSBillingConductorReadOnlyAccess	1461
使用此策略	1461
策略详细信息	1461
策略版本	1462
JSON 策略文档	1462
了解更多信息	1462
AWSBillingReadOnlyAccess	1462
使用此策略	1462
策略详细信息	1463
策略版本	1463
JSON 策略文档	1463
了解更多信息	1464
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	1465
使用此策略	1465
策略详细信息	1465
策略版本	1465
JSON 策略文档	1465
了解更多信息	1466
AWSBudgetsActionsWithAWSResourceControlAccess	1467
使用此策略	1467
策略详细信息	1467
策略版本	1467
JSON 策略文档	1467
了解更多信息	1468

AWSBudgetsReadOnlyAccess	1469
使用此策略	1469
策略详细信息	1469
策略版本	1469
JSON 策略文档	1469
了解更多信息	1470
AWSBugBustFullAccess	1470
使用此策略	1470
策略详细信息	1470
策略版本	1470
JSON 策略文档	1471
了解更多信息	1472
AWSBugBustPlayerAccess	1472
使用此策略	1472
策略详细信息	1472
策略版本	1472
JSON 策略文档	1472
了解更多信息	1473
AWSBugBustServiceRolePolicy	1474
使用此策略	1474
策略详细信息	1474
策略版本	1474
JSON 策略文档	1474
了解更多信息	1475
AWSCertificateManagerFullAccess	1475
使用此策略	1475
策略详细信息	1475
策略版本	1475
JSON 策略文档	1476
了解更多信息	1476
AWSCertificateManagerPrivateCAAuditor	1477
使用此策略	1477
策略详细信息	1477
策略版本	1477
JSON 策略文档	1477
了解更多信息	1478

AWSCertificateManagerPrivateCAFullAccess	1478
使用此策略	1478
策略详细信息	1478
策略版本	1479
JSON 策略文档	1479
了解更多信息	1479
AWSCertificateManagerPrivateCAPrivilegedUser	1479
使用此策略	1480
策略详细信息	1480
策略版本	1480
JSON 策略文档	1480
了解更多信息	1481
AWSCertificateManagerPrivateCAReadOnly	1481
使用此策略	1482
策略详细信息	1482
策略版本	1482
JSON 策略文档	1482
了解更多信息	1483
AWSCertificateManagerPrivateCAUser	1483
使用此策略	1483
策略详细信息	1483
策略版本	1483
JSON 策略文档	1483
了解更多信息	1485
AWSCertificateManagerReadOnly	1485
使用此策略	1485
策略详细信息	1485
策略版本	1485
JSON 策略文档	1485
了解更多信息	1486
AWSChatbotServiceLinkedRolePolicy	1486
使用此策略	1486
策略详细信息	1486
策略版本	1487
JSON 策略文档	1487
了解更多信息	1487

AWSCleanRoomsFullAccess	1488
使用此策略	1488
策略详细信息	1488
策略版本	1488
JSON 策略文档	1488
了解更多信息	1493
AWSCleanRoomsFullAccessNoQuerying	1493
使用此策略	1493
策略详细信息	1493
策略版本	1493
JSON 策略文档	1493
了解更多信息	1498
AWSCleanRoomsMLFullAccess	1498
使用此策略	1498
策略详细信息	1499
策略版本	1499
JSON 策略文档	1499
了解更多信息	1502
AWSCleanRoomsMLReadOnlyAccess	1503
使用此策略	1503
策略详细信息	1503
策略版本	1503
JSON 策略文档	1503
了解更多信息	1504
AWSCleanRoomsReadOnlyAccess	1504
使用此策略	1505
策略详细信息	1505
策略版本	1505
JSON 策略文档	1505
了解更多信息	1506
AWSCloud9Administrator	1506
使用此策略	1507
策略详细信息	1507
策略版本	1507
JSON 策略文档	1507
了解更多信息	1508

AWSCloud9EnvironmentMember	1509
使用此策略	1509
策略详细信息	1509
策略版本	1509
JSON 策略文档	1509
了解更多信息	1511
AWSCloud9ServiceRolePolicy	1511
使用此策略	1511
策略详细信息	1511
策略版本	1511
JSON 策略文档	1511
了解更多信息	1514
AWSCloud9SSMInstanceProfile	1514
使用此策略	1514
策略详细信息	1514
策略版本	1514
JSON 策略文档	1515
了解更多信息	1515
AWSCloud9User	1515
使用此策略	1515
策略详细信息	1515
策略版本	1516
JSON 策略文档	1516
了解更多信息	1518
AWSCloudFormationFullAccess	1518
使用此策略	1518
策略详细信息	1519
策略版本	1519
JSON 策略文档	1519
了解更多信息	1519
AWSCloudFormationReadOnlyAccess	1520
使用此策略	1520
策略详细信息	1520
策略版本	1520
JSON 策略文档	1520
了解更多信息	1521

AWSCloudFrontLogger	1521
使用此策略	1521
策略详细信息	1521
策略版本	1521
JSON 策略文档	1521
了解更多信息	1522
AWSCloudHSMFullAccess	1522
使用此策略	1522
策略详细信息	1522
策略版本	1522
JSON 策略文档	1523
了解更多信息	1523
AWSCloudHSMReadOnlyAccess	1523
使用此策略	1523
策略详细信息	1523
策略版本	1524
JSON 策略文档	1524
了解更多信息	1524
AWSCloudHSMRole	1524
使用此策略	1525
策略详细信息	1525
策略版本	1525
JSON 策略文档	1525
了解更多信息	1526
AWSCloudMapDiscoverInstanceAccess	1526
使用此策略	1526
策略详细信息	1526
策略版本	1526
JSON 策略文档	1526
了解更多信息	1527
AWSCloudMapFullAccess	1527
使用此策略	1527
策略详细信息	1527
策略版本	1528
JSON 策略文档	1528
了解更多信息	1528

AWSCloudMapReadOnlyAccess	1529
使用此策略	1529
策略详细信息	1529
策略版本	1529
JSON 策略文档	1529
了解更多信息	1530
AWSCloudMapRegisterInstanceAccess	1530
使用此策略	1530
策略详细信息	1530
策略版本	1530
JSON 策略文档	1531
了解更多信息	1531
AWSCloudShellFullAccess	1531
使用此策略	1532
策略详细信息	1532
策略版本	1532
JSON 策略文档	1532
了解更多信息	1532
AWSCloudTrail_FullAccess	1533
使用此策略	1533
策略详细信息	1533
策略版本	1533
JSON 策略文档	1533
了解更多信息	1536
AWSCloudTrail_ReadOnlyAccess	1536
使用此策略	1536
策略详细信息	1536
策略版本	1536
JSON 策略文档	1537
了解更多信息	1537
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	1537
使用此策略	1537
策略详细信息	1538
策略版本	1538
JSON 策略文档	1538
了解更多信息	1538

AWSCodeArtifactAdminAccess	1538
使用此策略	1539
策略详细信息	1539
策略版本	1539
JSON 策略文档	1539
了解更多信息	1540
AWSCodeArtifactReadOnlyAccess	1540
使用此策略	1540
策略详细信息	1540
策略版本	1540
JSON 策略文档	1540
了解更多信息	1541
AWSCodeBuildAdminAccess	1541
使用此策略	1542
策略详细信息	1542
策略版本	1542
JSON 策略文档	1542
了解更多信息	1545
AWSCodeBuildDeveloperAccess	1546
使用此策略	1546
策略详细信息	1546
策略版本	1546
JSON 策略文档	1546
了解更多信息	1549
AWSCodeBuildReadOnlyAccess	1549
使用此策略	1549
策略详细信息	1549
策略版本	1549
JSON 策略文档	1550
了解更多信息	1551
AWSCodeCommitFullAccess	1551
使用此策略	1551
策略详细信息	1552
策略版本	1552
JSON 策略文档	1552
了解更多信息	1556

AWSCodeCommitPowerUser	1557
使用此策略	1557
策略详细信息	1557
策略版本	1557
JSON 策略文档	1557
了解更多信息	1562
AWSCodeCommitReadOnly	1562
使用此策略	1562
策略详细信息	1562
策略版本	1563
JSON 策略文档	1563
了解更多信息	1565
AWSCodeDeployDeployerAccess	1566
使用此策略	1566
策略详细信息	1566
策略版本	1566
JSON 策略文档	1566
了解更多信息	1568
AWSCodeDeployFullAccess	1568
使用此策略	1568
策略详细信息	1568
策略版本	1568
JSON 策略文档	1568
了解更多信息	1570
AWSCodeDeployReadOnlyAccess	1570
使用此策略	1570
策略详细信息	1570
策略版本	1571
JSON 策略文档	1571
了解更多信息	1572
AWSCodeDeployRole	1572
使用此策略	1572
策略详细信息	1572
策略版本	1572
JSON 策略文档	1573
了解更多信息	1574

AWSCodeDeployRoleForCloudFormation	1574
使用此策略	1574
策略详细信息	1574
策略版本	1575
JSON 策略文档	1575
了解更多信息	1575
AWSCodeDeployRoleForECS	1575
使用此策略	1576
策略详细信息	1576
策略版本	1576
JSON 策略文档	1576
了解更多信息	1577
AWSCodeDeployRoleForECSLimited	1577
使用此策略	1577
策略详细信息	1577
策略版本	1578
JSON 策略文档	1578
了解更多信息	1580
AWSCodeDeployRoleForLambda	1580
使用此策略	1580
策略详细信息	1580
策略版本	1580
JSON 策略文档	1580
了解更多信息	1581
AWSCodeDeployRoleForLambdaLimited	1582
使用此策略	1582
策略详细信息	1582
策略版本	1582
JSON 策略文档	1582
了解更多信息	1583
AWSCodePipeline_FullAccess	1584
使用此策略	1584
策略详细信息	1584
策略版本	1584
JSON 策略文档	1584
了解更多信息	1588

AWSCodePipeline_ReadOnlyAccess	1588
使用此策略	1588
策略详细信息	1588
策略版本	1589
JSON 策略文档	1589
了解更多信息	1590
AWSCodePipelineApproverAccess	1590
使用此策略	1590
策略详细信息	1590
策略版本	1591
JSON 策略文档	1591
了解更多信息	1591
AWSCodePipelineCustomActionAccess	1591
使用此策略	1592
策略详细信息	1592
策略版本	1592
JSON 策略文档	1592
了解更多信息	1592
AWSCodeStarFullAccess	1593
使用此策略	1593
策略详细信息	1593
策略版本	1593
JSON 策略文档	1593
了解更多信息	1594
AWSCodeStarNotificationsServiceRolePolicy	1594
使用此策略	1594
策略详细信息	1595
策略版本	1595
JSON 策略文档	1595
了解更多信息	1596
AWSCodeStarServiceRole	1596
使用此策略	1596
策略详细信息	1597
策略版本	1597
JSON 策略文档	1597
了解更多信息	1602

AWSCompromisedKeyQuarantine	1602
使用此策略	1602
策略详细信息	1602
策略版本	1602
JSON 策略文档	1603
了解更多信息	1604
AWSCompromisedKeyQuarantineV2	1604
使用此策略	1604
策略详细信息	1604
策略版本	1604
JSON 策略文档	1604
了解更多信息	1606
AWSConfigMultiAccountSetupPolicy	1606
使用此策略	1607
策略详细信息	1607
策略版本	1607
JSON 策略文档	1607
了解更多信息	1609
AWSConfigRemediationServiceRolePolicy	1609
使用此策略	1609
策略详细信息	1609
策略版本	1610
JSON 策略文档	1610
了解更多信息	1610
AWSConfigRoleForOrganizations	1611
使用此策略	1611
策略详细信息	1611
策略版本	1611
JSON 策略文档	1611
了解更多信息	1612
AWSConfigRulesExecutionRole	1612
使用此策略	1612
策略详细信息	1612
策略版本	1612
JSON 策略文档	1612
了解更多信息	1613

AWSCONFIGServiceRolePolicy	1613
使用此策略	1613
策略详细信息	1614
策略版本	1614
JSON 策略文档	1614
了解更多信息	1645
AWSCONFIGUserAccess	1646
使用此策略	1646
策略详细信息	1646
策略版本	1646
JSON 策略文档	1646
了解更多信息	1647
AWSCONNECTOR	1647
使用此策略	1647
策略详细信息	1647
策略版本	1647
JSON 策略文档	1648
了解更多信息	1650
AWSCONTROLTowerAccountServiceRolePolicy	1650
使用此策略	1650
策略详细信息	1650
策略版本	1650
JSON 策略文档	1650
了解更多信息	1652
AWSCONTROLTowerServiceRolePolicy	1652
使用此策略	1652
策略详细信息	1652
策略版本	1653
JSON 策略文档	1653
了解更多信息	1657
AWSCOSTAndUsageReportAutomationPolicy	1658
使用此策略	1658
策略详细信息	1658
策略版本	1658
JSON 策略文档	1658
了解更多信息	1659

AWSDataExchangeFullAccess	1659
使用此策略	1660
策略详细信息	1660
策略版本	1660
JSON 策略文档	1660
了解更多信息	1663
AWSDataExchangeProviderFullAccess	1664
使用此策略	1664
策略详细信息	1664
策略版本	1664
JSON 策略文档	1664
了解更多信息	1668
AWSDataExchangeReadOnly	1668
使用此策略	1668
策略详细信息	1668
策略版本	1669
JSON 策略文档	1669
了解更多信息	1670
AWSDataExchangeSubscriberFullAccess	1670
使用此策略	1670
策略详细信息	1670
策略版本	1670
JSON 策略文档	1670
了解更多信息	1673
AWSDataLifecycleManagerServiceRole	1673
使用此策略	1673
策略详细信息	1673
策略版本	1673
JSON 策略文档	1673
了解更多信息	1675
AWSDataLifecycleManagerServiceRoleForAMIManagement	1675
使用此策略	1675
策略详细信息	1675
策略版本	1675
JSON 策略文档	1676
了解更多信息	1677

AWSDatalifecycleManagerSSMFullAccess	1677
使用此策略	1677
策略详细信息	1677
策略版本	1677
JSON 策略文档	1678
了解更多信息	1679
AWSDataPipeline_FullAccess	1679
使用此策略	1679
策略详细信息	1679
策略版本	1680
JSON 策略文档	1680
了解更多信息	1681
AWSDataPipeline_PowerUser	1681
使用此策略	1681
策略详细信息	1681
策略版本	1681
JSON 策略文档	1682
了解更多信息	1682
AWSDataSyncDiscoveryServiceRolePolicy	1683
使用此策略	1683
策略详细信息	1683
策略版本	1683
JSON 策略文档	1683
了解更多信息	1684
AWSDataSyncFullAccess	1684
使用此策略	1685
策略详细信息	1685
策略版本	1685
JSON 策略文档	1685
了解更多信息	1686
AWSDataSyncReadOnlyAccess	1687
使用此策略	1687
策略详细信息	1687
策略版本	1687
JSON 策略文档	1687
了解更多信息	1688

AWSDeadlineCloud-FleetWorker	1688
使用此策略	1688
策略详细信息	1688
策略版本	1688
JSON 策略文档	1689
了解更多信息	1689
AWSDeadlineCloud-UserAccessFarms	1689
使用此策略	1690
策略详细信息	1690
策略版本	1690
JSON 策略文档	1690
了解更多信息	1695
AWSDeadlineCloud-UserAccessFleets	1696
使用此策略	1696
策略详细信息	1696
策略版本	1696
JSON 策略文档	1696
了解更多信息	1700
AWSDeadlineCloud-UserAccessJobs	1700
使用此策略	1700
策略详细信息	1700
策略版本	1700
JSON 策略文档	1701
了解更多信息	1704
AWSDeadlineCloud-UserAccessQueues	1705
使用此策略	1705
策略详细信息	1705
策略版本	1705
JSON 策略文档	1705
了解更多信息	1710
AWSDeadlineCloud-WorkerHost	1710
使用此策略	1710
策略详细信息	1710
策略版本	1711
JSON 策略文档	1711
了解更多信息	1711

AWSDeepLensLambdaFunctionAccessPolicy	1711
使用此策略	1712
策略详细信息	1712
策略版本	1712
JSON 策略文档	1712
了解更多信息	1713
AWSDeepLensServiceRolePolicy	1714
使用此策略	1714
策略详细信息	1714
策略版本	1714
JSON 策略文档	1714
了解更多信息	1721
AWSDeepRacerAccountAdminAccess	1721
使用此策略	1722
策略详细信息	1722
策略版本	1722
JSON 策略文档	1722
了解更多信息	1723
AWSDeepRacerCloudFormationAccessPolicy	1723
使用此策略	1723
策略详细信息	1723
策略版本	1723
JSON 策略文档	1723
了解更多信息	1726
AWSDeepRacerDefaultMultiUserAccess	1726
使用此策略	1727
策略详细信息	1727
策略版本	1727
JSON 策略文档	1727
了解更多信息	1728
AWSDeepRacerFullAccess	1729
使用此策略	1729
策略详细信息	1729
策略版本	1729
JSON 策略文档	1729
了解更多信息	1730

AWSDeepRacerRoboMakerAccessPolicy	1730
使用此策略	1731
策略详细信息	1731
策略版本	1731
JSON 策略文档	1731
了解更多信息	1733
AWSDeepRacerServiceRolePolicy	1733
使用此策略	1733
策略详细信息	1733
策略版本	1734
JSON 策略文档	1734
了解更多信息	1737
AWSDenyAll	1737
使用此策略	1737
策略详细信息	1737
策略版本	1737
JSON 策略文档	1738
了解更多信息	1738
AWSDeviceFarmFullAccess	1738
使用此策略	1738
策略详细信息	1738
策略版本	1739
JSON 策略文档	1739
了解更多信息	1739
AWSDeviceFarmServiceRolePolicy	1739
使用此策略	1740
策略详细信息	1740
策略版本	1740
JSON 策略文档	1740
了解更多信息	1742
AWSDeviceFarmTestGridServiceRolePolicy	1742
使用此策略	1742
策略详细信息	1743
策略版本	1743
JSON 策略文档	1743
了解更多信息	1745

AWSDirectConnectFullAccess	1745
使用此策略	1745
策略详细信息	1745
策略版本	1746
JSON 策略文档	1746
了解更多信息	1746
AWSDirectConnectReadOnlyAccess	1746
使用此策略	1747
策略详细信息	1747
策略版本	1747
JSON 策略文档	1747
了解更多信息	1747
AWSDirectConnectServiceRolePolicy	1748
使用此策略	1748
策略详细信息	1748
策略版本	1748
JSON 策略文档	1748
了解更多信息	1749
AWSDirectoryServiceFullAccess	1749
使用此策略	1749
策略详细信息	1749
策略版本	1749
JSON 策略文档	1750
了解更多信息	1751
AWSDirectoryServiceReadOnlyAccess	1752
使用此策略	1752
策略详细信息	1752
策略版本	1752
JSON 策略文档	1752
了解更多信息	1753
AWSDiscoveryContinuousExportFirehosePolicy	1753
使用此策略	1753
策略详细信息	1753
策略版本	1754
JSON 策略文档	1754
了解更多信息	1755

AWSDMSFleetAdvisorServiceRolePolicy	1755
使用此策略	1755
策略详细信息	1755
策略版本	1755
JSON 策略文档	1756
了解更多信息	1756
AWSDMSServerlessServiceRolePolicy	1756
使用此策略	1756
策略详细信息	1756
策略版本	1757
JSON 策略文档	1757
了解更多信息	1758
AWSEC2CapacityReservationFleetRolePolicy	1758
使用此策略	1758
策略详细信息	1759
策略版本	1759
JSON 策略文档	1759
了解更多信息	1760
AWSEC2FleetServiceRolePolicy	1760
使用此策略	1760
策略详细信息	1760
策略版本	1761
JSON 策略文档	1761
了解更多信息	1763
AWSEC2SpotFleetServiceRolePolicy	1763
使用此策略	1763
策略详细信息	1763
策略版本	1763
JSON 策略文档	1764
了解更多信息	1765
AWSEC2SpotServiceRolePolicy	1766
使用此策略	1766
策略详细信息	1766
策略版本	1766
JSON 策略文档	1766
了解更多信息	1768

AWSEC2VssSnapshotPolicy	1768
使用此策略	1768
策略详细信息	1768
策略版本	1768
JSON 策略文档	1768
了解更多信息	1772
AWSECRPullThroughCache_ServiceRolePolicy	1772
使用此策略	1772
策略详细信息	1772
策略版本	1772
JSON 策略文档	1773
了解更多信息	1773
AWSElasticBeanstalkCustomPlatformforEC2Role	1774
使用此策略	1774
策略详细信息	1774
策略版本	1774
JSON 策略文档	1774
了解更多信息	1776
AWSElasticBeanstalkEnhancedHealth	1776
使用此策略	1776
策略详细信息	1776
策略版本	1777
JSON 策略文档	1777
了解更多信息	1778
AWSElasticBeanstalkMaintenance	1778
使用此策略	1778
策略详细信息	1778
策略版本	1778
JSON 策略文档	1779
了解更多信息	1779
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	1779
使用此策略	1780
策略详细信息	1780
策略版本	1780
JSON 策略文档	1780
了解更多信息	1787

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	1787
使用此策略	1787
策略详细信息	1787
策略版本	1788
JSON 策略文档	1788
了解更多信息	1793
AWSElasticBeanstalkMulticontainerDocker	1793
使用此策略	1793
策略详细信息	1793
策略版本	1794
JSON 策略文档	1794
了解更多信息	1795
AWSElasticBeanstalkReadOnly	1795
使用此策略	1795
策略详细信息	1795
策略版本	1795
JSON 策略文档	1796
了解更多信息	1798
AWSElasticBeanstalkRoleCore	1798
使用此策略	1798
策略详细信息	1798
策略版本	1798
JSON 策略文档	1799
了解更多信息	1803
AWSElasticBeanstalkRoleCWL	1804
使用此策略	1804
策略详细信息	1804
策略版本	1804
JSON 策略文档	1804
了解更多信息	1805
AWSElasticBeanstalkRoleECS	1805
使用此策略	1805
策略详细信息	1805
策略版本	1805
JSON 策略文档	1806
了解更多信息	1806

AWSElasticBeanstalkRoleRDS	1807
使用此策略	1807
策略详细信息	1807
策略版本	1807
JSON 策略文档	1807
了解更多信息	1808
AWSElasticBeanstalkRoleSNS	1808
使用此策略	1808
策略详细信息	1808
策略版本	1808
JSON 策略文档	1809
了解更多信息	1809
AWSElasticBeanstalkRoleWorkerTier	1810
使用此策略	1810
策略详细信息	1810
策略版本	1810
JSON 策略文档	1810
了解更多信息	1811
AWSElasticBeanstalkService	1811
使用此策略	1811
策略详细信息	1811
策略版本	1812
JSON 策略文档	1812
了解更多信息	1816
AWSElasticBeanstalkServiceRolePolicy	1816
使用此策略	1816
策略详细信息	1817
策略版本	1817
JSON 策略文档	1817
了解更多信息	1818
AWSElasticBeanstalkWebTier	1819
使用此策略	1819
策略详细信息	1819
策略版本	1819
JSON 策略文档	1819
了解更多信息	1821

AWSElasticBeanstalkWorkerTier	1821
使用此策略	1821
策略详细信息	1821
策略版本	1821
JSON 策略文档	1821
了解更多信息	1824
AWSElasticDisasterRecoveryAgentInstallationPolicy	1824
使用此策略	1824
策略详细信息	1824
策略版本	1824
JSON 策略文档	1824
了解更多信息	1826
AWSElasticDisasterRecoveryAgentPolicy	1826
使用此策略	1826
策略详细信息	1826
策略版本	1827
JSON 策略文档	1827
了解更多信息	1828
AWSElasticDisasterRecoveryConsoleFullAccess	1828
使用此策略	1828
策略详细信息	1828
策略版本	1828
JSON 策略文档	1828
了解更多信息	1838
AWSElasticDisasterRecoveryConsoleFullAccess_v2	1838
使用此策略	1839
策略详细信息	1839
策略版本	1839
JSON 策略文档	1839
了解更多信息	1852
AWSElasticDisasterRecoveryConversionServerPolicy	1852
使用此策略	1852
策略详细信息	1852
策略版本	1852
JSON 策略文档	1853
了解更多信息	1853

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	1853
使用此策略	1854
策略详细信息	1854
策略版本	1854
JSON 策略文档	1854
了解更多信息	1855
AWSElasticDisasterRecoveryEc2InstancePolicy	1855
使用此策略	1855
策略详细信息	1855
策略版本	1856
JSON 策略文档	1856
了解更多信息	1858
AWSElasticDisasterRecoveryFailbackInstallationPolicy	1858
使用此策略	1858
策略详细信息	1858
策略版本	1859
JSON 策略文档	1859
了解更多信息	1859
AWSElasticDisasterRecoveryFailbackPolicy	1860
使用此策略	1860
策略详细信息	1860
策略版本	1860
JSON 策略文档	1860
了解更多信息	1862
AWSElasticDisasterRecoveryLaunchActionsPolicy	1862
使用此策略	1862
策略详细信息	1862
策略版本	1862
JSON 策略文档	1862
了解更多信息	1868
AWSElasticDisasterRecoveryNetworkReplicationPolicy	1869
使用此策略	1869
策略详细信息	1869
策略版本	1869
JSON 策略文档	1869
了解更多信息	1870

AWSElasticDisasterRecoveryReadOnlyAccess	1870
使用此策略	1870
策略详细信息	1870
策略版本	1871
JSON 策略文档	1871
了解更多信息	1873
AWSElasticDisasterRecoveryRecoveryInstancePolicy	1873
使用此策略	1873
策略详细信息	1873
策略版本	1874
JSON 策略文档	1874
了解更多信息	1876
AWSElasticDisasterRecoveryReplicationServerPolicy	1876
使用此策略	1877
策略详细信息	1877
策略版本	1877
JSON 策略文档	1877
了解更多信息	1879
AWSElasticDisasterRecoveryServiceRolePolicy	1880
使用此策略	1880
策略详细信息	1880
策略版本	1880
JSON 策略文档	1880
了解更多信息	1889
AWSElasticDisasterRecoveryStagingAccountPolicy	1889
使用此策略	1889
策略详细信息	1889
策略版本	1889
JSON 策略文档	1889
了解更多信息	1890
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	1891
使用此策略	1891
策略详细信息	1891
策略版本	1891
JSON 策略文档	1891
了解更多信息	1892

AWSElasticLoadBalancingClassicServiceRolePolicy	1893
使用此策略	1893
策略详细信息	1893
策略版本	1893
JSON 策略文档	1893
了解更多信息	1894
AWSElasticLoadBalancingServiceRolePolicy	1894
使用此策略	1894
策略详细信息	1894
策略版本	1895
JSON 策略文档	1895
了解更多信息	1896
AWSElementalMediaConvertFullAccess	1896
使用此策略	1896
策略详细信息	1896
策略版本	1897
JSON 策略文档	1897
了解更多信息	1897
AWSElementalMediaConvertReadOnly	1898
使用此策略	1898
策略详细信息	1898
策略版本	1898
JSON 策略文档	1898
了解更多信息	1899
AWSElementalMediaLiveFullAccess	1899
使用此策略	1899
策略详细信息	1899
策略版本	1899
JSON 策略文档	1900
了解更多信息	1900
AWSElementalMediaLiveReadOnly	1900
使用此策略	1900
策略详细信息	1900
策略版本	1901
JSON 策略文档	1901
了解更多信息	1901

AWSElementalMediaPackageFullAccess	1901
使用此策略	1901
策略详细信息	1902
策略版本	1902
JSON 策略文档	1902
了解更多信息	1902
AWSElementalMediaPackageReadOnly	1902
使用此策略	1903
策略详细信息	1903
策略版本	1903
JSON 策略文档	1903
了解更多信息	1903
AWSElementalMediaPackageV2FullAccess	1904
使用此策略	1904
策略详细信息	1904
策略版本	1904
JSON 策略文档	1904
了解更多信息	1904
AWSElementalMediaPackageV2ReadOnly	1905
使用此策略	1905
策略详细信息	1905
策略版本	1905
JSON 策略文档	1905
了解更多信息	1906
AWSElementalMediaStoreFullAccess	1906
使用此策略	1906
策略详细信息	1906
策略版本	1906
JSON 策略文档	1906
了解更多信息	1907
AWSElementalMediaStoreReadOnly	1907
使用此策略	1907
策略详细信息	1907
策略版本	1908
JSON 策略文档	1908
了解更多信息	1908

AWSElementalMediaTailorFullAccess	1908
使用此策略	1909
策略详细信息	1909
策略版本	1909
JSON 策略文档	1909
了解更多信息	1909
AWSElementalMediaTailorReadOnly	1910
使用此策略	1910
策略详细信息	1910
策略版本	1910
JSON 策略文档	1910
了解更多信息	1911
AWSEnhancedClassicNetworkingMangementPolicy	1911
使用此策略	1911
策略详细信息	1911
策略版本	1911
JSON 策略文档	1911
了解更多信息	1912
AWSEntityResolutionConsoleFullAccess	1912
使用此策略	1912
策略详细信息	1912
策略版本	1912
JSON 策略文档	1913
了解更多信息	1915
AWSEntityResolutionConsoleReadOnlyAccess	1915
使用此策略	1916
策略详细信息	1916
策略版本	1916
JSON 策略文档	1916
了解更多信息	1916
AWSFaultInjectionSimulatorEC2Access	1917
使用此策略	1917
策略详细信息	1917
策略版本	1917
JSON 策略文档	1917
了解更多信息	1919

AWSFaultInjectionSimulatorECSAccess	1919
使用此策略	1919
策略详细信息	1919
策略版本	1920
JSON 策略文档	1920
了解更多信息	1921
AWSFaultInjectionSimulatorEKSAccess	1922
使用此策略	1922
策略详细信息	1922
策略版本	1922
JSON 策略文档	1922
了解更多信息	1923
AWSFaultInjectionSimulatorNetworkAccess	1924
使用此策略	1924
策略详细信息	1924
策略版本	1924
JSON 策略文档	1924
了解更多信息	1931
AWSFaultInjectionSimulatorRDSAccess	1931
使用此策略	1931
策略详细信息	1932
策略版本	1932
JSON 策略文档	1932
了解更多信息	1933
AWSFaultInjectionSimulatorSSMAccess	1933
使用此策略	1933
策略详细信息	1933
策略版本	1934
JSON 策略文档	1934
了解更多信息	1935
AWSFinSpaceServiceRolePolicy	1935
使用此策略	1935
策略详细信息	1936
策略版本	1936
JSON 策略文档	1936
了解更多信息	1936

AWSFMAdminFullAccess	1937
使用此策略	1937
策略详细信息	1937
策略版本	1937
JSON 策略文档	1937
了解更多信息	1939
AWSFMAdminReadOnlyAccess	1939
使用此策略	1939
策略详细信息	1939
策略版本	1940
JSON 策略文档	1940
了解更多信息	1941
AWSFMMemberReadOnlyAccess	1942
使用此策略	1942
策略详细信息	1942
策略版本	1942
JSON 策略文档	1942
了解更多信息	1943
AWSForWordPressPluginPolicy	1943
使用此策略	1943
策略详细信息	1943
策略版本	1943
JSON 策略文档	1944
了解更多信息	1945
AWSGitSyncServiceRolePolicy	1946
使用此策略	1946
策略详细信息	1946
策略版本	1946
JSON 策略文档	1946
了解更多信息	1947
AWSGlobalAcceleratorSLRPolicy	1947
使用此策略	1947
策略详细信息	1947
策略版本	1947
JSON 策略文档	1948
了解更多信息	1949

AWSGlueConsoleFullAccess	1949
使用此策略	1949
策略详细信息	1950
策略版本	1950
JSON 策略文档	1950
了解更多信息	1954
AWSGlueConsoleSageMakerNotebookFullAccess	1954
使用此策略	1954
策略详细信息	1955
策略版本	1955
JSON 策略文档	1955
了解更多信息	1960
AwsGlueDataBrewFullAccessPolicy	1960
使用此策略	1960
策略详细信息	1961
策略版本	1961
JSON 策略文档	1961
了解更多信息	1966
AWSGlueDataBrewServiceRole	1966
使用此策略	1966
策略详细信息	1966
策略版本	1967
JSON 策略文档	1967
了解更多信息	1970
AWSGlueSchemaRegistryFullAccess	1970
使用此策略	1970
策略详细信息	1970
策略版本	1970
JSON 策略文档	1970
了解更多信息	1972
AWSGlueSchemaRegistryReadOnlyAccess	1972
使用此策略	1972
策略详细信息	1972
策略版本	1972
JSON 策略文档	1972
了解更多信息	1973

AWSGlueServiceNotebookRole	1973
使用此策略	1973
策略详细信息	1974
策略版本	1974
JSON 策略文档	1974
了解更多信息	1976
AWSGlueServiceRole	1976
使用此策略	1977
策略详细信息	1977
策略版本	1977
JSON 策略文档	1977
了解更多信息	1979
AwsGlueSessionUserRestrictedNotebookPolicy	1979
使用此策略	1980
策略详细信息	1980
策略版本	1980
JSON 策略文档	1980
了解更多信息	1983
AwsGlueSessionUserRestrictedNotebookServiceRole	1983
使用此策略	1983
策略详细信息	1983
策略版本	1983
JSON 策略文档	1983
了解更多信息	1987
AwsGlueSessionUserRestrictedPolicy	1987
使用此策略	1987
策略详细信息	1988
策略版本	1988
JSON 策略文档	1988
了解更多信息	1990
AwsGlueSessionUserRestrictedServiceRole	1991
使用此策略	1991
策略详细信息	1991
策略版本	1991
JSON 策略文档	1991
了解更多信息	1995

AWSGrafanaAccountAdministrator	1995
使用此策略	1996
策略详细信息	1996
策略版本	1996
JSON 策略文档	1996
了解更多信息	1997
AWSGrafanaConsoleReadOnlyAccess	1997
使用此策略	1997
策略详细信息	1997
策略版本	1998
JSON 策略文档	1998
了解更多信息	1998
AWSGrafanaWorkspacePermissionManagement	1998
使用此策略	1999
策略详细信息	1999
策略版本	1999
JSON 策略文档	1999
了解更多信息	2000
AWSGrafanaWorkspacePermissionManagementV2	2000
使用此策略	2000
策略详细信息	2000
策略版本	2001
JSON 策略文档	2001
了解更多信息	2002
AWSGreengrassFullAccess	2002
使用此策略	2002
策略详细信息	2002
策略版本	2002
JSON 策略文档	2003
了解更多信息	2003
AWSGreengrassReadOnlyAccess	2003
使用此策略	2003
策略详细信息	2003
策略版本	2004
JSON 策略文档	2004
了解更多信息	2004

AWSGreengrassResourceAccessRolePolicy	2004
使用此策略	2004
策略详细信息	2005
策略版本	2005
JSON 策略文档	2005
了解更多信息	2007
AWSGroundStationAgentInstancePolicy	2007
使用此策略	2008
策略详细信息	2008
策略版本	2008
JSON 策略文档	2008
了解更多信息	2008
AWSHealth_EventProcessorServiceRolePolicy	2009
使用此策略	2009
策略详细信息	2009
策略版本	2009
JSON 策略文档	2009
了解更多信息	2010
AWSHealthFullAccess	2010
使用此策略	2010
策略详细信息	2010
策略版本	2011
JSON 策略文档	2011
了解更多信息	2012
AWSHealthImagingFullAccess	2012
使用此策略	2012
策略详细信息	2012
策略版本	2012
JSON 策略文档	2013
了解更多信息	2013
AWSHealthImagingReadOnlyAccess	2013
使用此策略	2014
策略详细信息	2014
策略版本	2014
JSON 策略文档	2014
了解更多信息	2015

AWSIAMIdentityCenterAllowListForIdentityContext	2015
使用此策略	2015
策略详细信息	2015
策略版本	2015
JSON 策略文档	2016
了解更多信息	2018
AWSIdentitySyncFullAccess	2018
使用此策略	2019
策略详细信息	2019
策略版本	2019
JSON 策略文档	2019
了解更多信息	2020
AWSIdentitySyncReadOnlyAccess	2020
使用此策略	2020
策略详细信息	2020
策略版本	2021
JSON 策略文档	2021
了解更多信息	2021
AWSImageBuilderFullAccess	2021
使用此策略	2022
策略详细信息	2022
策略版本	2022
JSON 策略文档	2022
了解更多信息	2025
AWSImageBuilderReadOnlyAccess	2025
使用此策略	2025
策略详细信息	2025
策略版本	2025
JSON 策略文档	2026
了解更多信息	2026
AWSImportExportFullAccess	2026
使用此策略	2026
策略详细信息	2027
策略版本	2027
JSON 策略文档	2027
了解更多信息	2027

AWSImportExportReadOnlyAccess	2028
使用此策略	2028
策略详细信息	2028
策略版本	2028
JSON 策略文档	2028
了解更多信息	2029
AWSIncidentManagerIncidentAccessServiceRolePolicy	2029
使用此策略	2029
策略详细信息	2029
策略版本	2029
JSON 策略文档	2029
了解更多信息	2030
AWSIncidentManagerResolverAccess	2030
使用此策略	2030
策略详细信息	2030
策略版本	2031
JSON 策略文档	2031
了解更多信息	2032
AWSIncidentManagerServiceRolePolicy	2032
使用此策略	2032
策略详细信息	2032
策略版本	2032
JSON 策略文档	2033
了解更多信息	2034
AWSIoT1ClickFullAccess	2034
使用此策略	2034
策略详细信息	2034
策略版本	2034
JSON 策略文档	2034
了解更多信息	2035
AWSIoT1ClickReadOnlyAccess	2035
使用此策略	2035
策略详细信息	2035
策略版本	2035
JSON 策略文档	2036
了解更多信息	2036

AWSIoTAnalyticsFullAccess	2036
使用此策略	2036
策略详细信息	2036
策略版本	2037
JSON 策略文档	2037
了解更多信息	2037
AWSIoTAnalyticsReadOnlyAccess	2037
使用此策略	2038
策略详细信息	2038
策略版本	2038
JSON 策略文档	2038
了解更多信息	2038
AWSIoTConfigAccess	2039
使用此策略	2039
策略详细信息	2039
策略版本	2039
JSON 策略文档	2039
了解更多信息	2043
AWSIoTConfigReadOnlyAccess	2043
使用此策略	2043
策略详细信息	2044
策略版本	2044
JSON 策略文档	2044
了解更多信息	2046
AWSIoTDataAccess	2046
使用此策略	2046
策略详细信息	2046
策略版本	2047
JSON 策略文档	2047
了解更多信息	2047
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	2047
使用此策略	2048
策略详细信息	2048
策略版本	2048
JSON 策略文档	2048
了解更多信息	2049

AWSIoTDeviceDefenderAudit	2049
使用此策略	2049
策略详细信息	2049
策略版本	2049
JSON 策略文档	2049
了解更多信息	2050
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	2050
使用此策略	2051
策略详细信息	2051
策略版本	2051
JSON 策略文档	2051
了解更多信息	2052
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	2052
使用此策略	2052
策略详细信息	2052
策略版本	2053
JSON 策略文档	2053
了解更多信息	2053
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	2053
使用此策略	2054
策略详细信息	2054
策略版本	2054
JSON 策略文档	2054
了解更多信息	2055
AWSIoTDeviceDefenderUpdateCACertMitigationAction	2055
使用此策略	2055
策略详细信息	2055
策略版本	2055
JSON 策略文档	2055
了解更多信息	2056
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	2056
使用此策略	2056
策略详细信息	2056
策略版本	2057
JSON 策略文档	2057
了解更多信息	2057

AWSIoTDeviceTesterForFreeRTOSFullAccess	2057
使用此策略	2058
策略详细信息	2058
策略版本	2058
JSON 策略文档	2058
了解更多信息	2064
AWSIoTDeviceTesterForGreengrassFullAccess	2064
使用此策略	2065
策略详细信息	2065
策略版本	2065
JSON 策略文档	2065
了解更多信息	2068
AWSIoTEventsFullAccess	2068
使用此策略	2068
策略详细信息	2068
策略版本	2069
JSON 策略文档	2069
了解更多信息	2069
AWSIoTEventsReadOnlyAccess	2069
使用此策略	2069
策略详细信息	2070
策略版本	2070
JSON 策略文档	2070
了解更多信息	2070
AWSIoTFleetHubFederationAccess	2071
使用此策略	2071
策略详细信息	2071
策略版本	2071
JSON 策略文档	2071
了解更多信息	2073
AWSIoTFleetwiseServiceRolePolicy	2073
使用此策略	2073
策略详细信息	2073
策略版本	2074
JSON 策略文档	2074
了解更多信息	2074

AWSIoTFullAccess	2074
使用此策略	2075
策略详细信息	2075
策略版本	2075
JSON 策略文档	2075
了解更多信息	2075
AWSIoTLogging	2076
使用此策略	2076
策略详细信息	2076
策略版本	2076
JSON 策略文档	2076
了解更多信息	2077
AWSIoTOTAUpdate	2077
使用此策略	2077
策略详细信息	2077
策略版本	2077
JSON 策略文档	2078
了解更多信息	2078
AWSIoTRoboRunnerFullAccess	2078
使用此策略	2078
策略详细信息	2078
策略版本	2079
JSON 策略文档	2079
了解更多信息	2079
AWSIoTRoboRunnerReadOnly	2080
使用此策略	2080
策略详细信息	2080
策略版本	2080
JSON 策略文档	2080
了解更多信息	2081
AWSIoTRoboRunnerServiceRolePolicy	2081
使用此策略	2081
策略详细信息	2081
策略版本	2081
JSON 策略文档	2082
了解更多信息	2082

AWSIoTRuleActions	2082
使用此策略	2082
策略详细信息	2082
策略版本	2083
JSON 策略文档	2083
了解更多信息	2083
AWSIoTSiteWiseConsoleFullAccess	2084
使用此策略	2084
策略详细信息	2084
策略版本	2084
JSON 策略文档	2084
了解更多信息	2086
AWSIoTSiteWiseFullAccess	2086
使用此策略	2087
策略详细信息	2087
策略版本	2087
JSON 策略文档	2087
了解更多信息	2087
AWSIoTSiteWiseMonitorPortalAccess	2088
使用此策略	2088
策略详细信息	2088
策略版本	2088
JSON 策略文档	2088
了解更多信息	2089
AWSIoTSiteWiseMonitorServiceRolePolicy	2090
使用此策略	2090
策略详细信息	2090
策略版本	2090
JSON 策略文档	2090
了解更多信息	2091
AWSIoTSiteWiseReadOnlyAccess	2091
使用此策略	2091
策略详细信息	2092
策略版本	2092
JSON 策略文档	2092
了解更多信息	2092

AWSIoTThingsRegistration	2093
使用此策略	2093
策略详细信息	2093
策略版本	2093
JSON 策略文档	2093
了解更多信息	2094
AWSIoTTwinMakerServiceRolePolicy	2094
使用此策略	2095
策略详细信息	2095
策略版本	2095
JSON 策略文档	2095
了解更多信息	2097
AWSIoTWirelessDataAccess	2097
使用此策略	2097
策略详细信息	2097
策略版本	2097
JSON 策略文档	2097
了解更多信息	2098
AWSIoTWirelessFullAccess	2098
使用此策略	2098
策略详细信息	2098
策略版本	2098
JSON 策略文档	2099
了解更多信息	2099
AWSIoTWirelessFullPublishAccess	2099
使用此策略	2099
策略详细信息	2099
策略版本	2100
JSON 策略文档	2100
了解更多信息	2100
AWSIoTWirelessGatewayCertManager	2100
使用此策略	2101
策略详细信息	2101
策略版本	2101
JSON 策略文档	2101
了解更多信息	2101

AWSIoTWirelessLogging	2102
使用此策略	2102
策略详细信息	2102
策略版本	2102
JSON 策略文档	2102
了解更多信息	2103
AWSIoTWirelessReadOnlyAccess	2103
使用此策略	2103
策略详细信息	2103
策略版本	2103
JSON 策略文档	2104
了解更多信息	2104
AWSIPAMServiceRolePolicy	2104
使用此策略	2104
策略详细信息	2104
策略版本	2105
JSON 策略文档	2105
了解更多信息	2106
AWSIQContractServiceRolePolicy	2106
使用此策略	2106
策略详细信息	2106
策略版本	2106
JSON 策略文档	2107
了解更多信息	2107
AWSIQFullAccess	2107
使用此策略	2107
策略详细信息	2107
策略版本	2108
JSON 策略文档	2108
了解更多信息	2108
AWSIQPermissionServiceRolePolicy	2109
使用此策略	2109
策略详细信息	2109
策略版本	2109
JSON 策略文档	2109
了解更多信息	2110

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2110
使用此策略	2110
策略详细信息	2110
策略版本	2111
JSON 策略文档	2111
了解更多信息	2111
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2112
使用此策略	2112
策略详细信息	2112
策略版本	2112
JSON 策略文档	2112
了解更多信息	2113
AWSKeyManagementServicePowerUser	2113
使用此策略	2113
策略详细信息	2113
策略版本	2113
JSON 策略文档	2113
了解更多信息	2114
AWSLakeFormationCrossAccountManager	2114
使用此策略	2114
策略详细信息	2114
策略版本	2115
JSON 策略文档	2115
了解更多信息	2117
AWSLakeFormationDataAdmin	2117
使用此策略	2117
策略详细信息	2117
策略版本	2117
JSON 策略文档	2118
了解更多信息	2119
AWSLambda_FullAccess	2119
使用此策略	2119
策略详细信息	2119
策略版本	2120
JSON 策略文档	2120
了解更多信息	2121

AWSLambda_ReadOnlyAccess	2121
使用此策略	2121
策略详细信息	2121
策略版本	2122
JSON 策略文档	2122
了解更多信息	2123
AWSLambdaBasicExecutionRole	2123
使用此策略	2123
策略详细信息	2124
策略版本	2124
JSON 策略文档	2124
了解更多信息	2124
AWSLambdaDynamoDBExecutionRole	2125
使用此策略	2125
策略详细信息	2125
策略版本	2125
JSON 策略文档	2125
了解更多信息	2126
AWSLambdaENIManagementAccess	2126
使用此策略	2126
策略详细信息	2126
策略版本	2126
JSON 策略文档	2127
了解更多信息	2127
AWSLambdaExecute	2127
使用此策略	2127
策略详细信息	2127
策略版本	2128
JSON 策略文档	2128
了解更多信息	2128
AWSLambdaFullAccess	2129
使用此策略	2129
策略详细信息	2129
策略版本	2129
JSON 策略文档	2129
了解更多信息	2131

AWSLambdaInvocation-DynamoDB	2131
使用此策略	2131
策略详细信息	2131
策略版本	2131
JSON 策略文档	2132
了解更多信息	2132
AWSLambdaKinesisExecutionRole	2132
使用此策略	2133
策略详细信息	2133
策略版本	2133
JSON 策略文档	2133
了解更多信息	2134
AWSLambdaMSKExecutionRole	2134
使用此策略	2134
策略详细信息	2134
策略版本	2134
JSON 策略文档	2134
了解更多信息	2135
AWSLambdaReplicator	2135
使用此策略	2135
策略详细信息	2136
策略版本	2136
JSON 策略文档	2136
了解更多信息	2137
AWSLambdaRole	2137
使用此策略	2137
策略详细信息	2137
策略版本	2138
JSON 策略文档	2138
了解更多信息	2138
AWSLambdaSQSQueueExecutionRole	2138
使用此策略	2139
策略详细信息	2139
策略版本	2139
JSON 策略文档	2139
了解更多信息	2140

AWSLambdaVPCAccessExecutionRole	2140
使用此策略	2140
策略详细信息	2140
策略版本	2140
JSON 策略文档	2140
了解更多信息	2141
AWSLicenseManagerConsumptionPolicy	2141
使用此策略	2141
策略详细信息	2141
策略版本	2142
JSON 策略文档	2142
了解更多信息	2142
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	2142
使用此策略	2143
策略详细信息	2143
策略版本	2143
JSON 策略文档	2143
了解更多信息	2144
AWSLicenseManagerMasterAccountRolePolicy	2144
使用此策略	2144
策略详细信息	2144
策略版本	2145
JSON 策略文档	2145
了解更多信息	2150
AWSLicenseManagerMemberAccountRolePolicy	2150
使用此策略	2150
策略详细信息	2150
策略版本	2150
JSON 策略文档	2150
了解更多信息	2151
AWSLicenseManagerServiceRolePolicy	2152
使用此策略	2152
策略详细信息	2152
策略版本	2152
JSON 策略文档	2152
了解更多信息	2155

AWSLicenseManagerUserSubscriptionsServiceRolePolicy	2156
使用此策略	2156
策略详细信息	2156
策略版本	2156
JSON 策略文档	2156
了解更多信息	2158
AWSM2ServicePolicy	2158
使用此策略	2158
策略详细信息	2158
策略版本	2159
JSON 策略文档	2159
了解更多信息	2160
AWSManagedServices_ContactsServiceRolePolicy	2160
使用此策略	2160
策略详细信息	2161
策略版本	2161
JSON 策略文档	2161
了解更多信息	2162
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	2162
使用此策略	2162
策略详细信息	2162
策略版本	2162
JSON 策略文档	2163
了解更多信息	2164
AWSManagedServices_EventsServiceRolePolicy	2164
使用此策略	2164
策略详细信息	2164
策略版本	2165
JSON 策略文档	2165
了解更多信息	2166
AWSManagedServicesDeploymentToolkitPolicy	2166
使用此策略	2166
策略详细信息	2166
策略版本	2166
JSON 策略文档	2166
了解更多信息	2168

AWSMarketplaceAmiIngestion	2169
使用此策略	2169
策略详细信息	2169
策略版本	2169
JSON 策略文档	2169
了解更多信息	2170
AWSMarketplaceDeploymentServiceRolePolicy	2170
使用此策略	2170
策略详细信息	2170
策略版本	2170
JSON 策略文档	2171
了解更多信息	2172
AWSMarketplaceFullAccess	2172
使用此策略	2172
策略详细信息	2172
策略版本	2173
JSON 策略文档	2173
了解更多信息	2176
AWSMarketplaceGetEntitlements	2176
使用此策略	2176
策略详细信息	2176
策略版本	2177
JSON 策略文档	2177
了解更多信息	2177
AWSMarketplaceImageBuildFullAccess	2177
使用此策略	2177
策略详细信息	2178
策略版本	2178
JSON 策略文档	2178
了解更多信息	2181
AWSMarketplaceLicenseManagementServiceRolePolicy	2182
使用此策略	2182
策略详细信息	2182
策略版本	2182
JSON 策略文档	2182
了解更多信息	2183

AWSMarketplaceManageSubscriptions	2183
使用此策略	2183
策略详细信息	2183
策略版本	2183
JSON 策略文档	2184
了解更多信息	2184
AWSMarketplaceMeteringFullAccess	2185
使用此策略	2185
策略详细信息	2185
策略版本	2185
JSON 策略文档	2185
了解更多信息	2186
AWSMarketplaceMeteringRegisterUsage	2186
使用此策略	2186
策略详细信息	2186
策略版本	2186
JSON 策略文档	2186
了解更多信息	2187
AWSMarketplaceProcurementSystemAdminFullAccess	2187
使用此策略	2187
策略详细信息	2187
策略版本	2188
JSON 策略文档	2188
了解更多信息	2188
AWSMarketplacePurchaseOrdersServiceRolePolicy	2188
使用此策略	2189
策略详细信息	2189
策略版本	2189
JSON 策略文档	2189
了解更多信息	2190
AWSMarketplaceRead-only	2190
使用此策略	2190
策略详细信息	2190
策略版本	2190
JSON 策略文档	2190
了解更多信息	2191

AWSMarketplaceResaleAuthorizationServiceRolePolicy	2192
使用此策略	2192
策略详细信息	2192
策略版本	2192
JSON 策略文档	2192
了解更多信息	2195
AWSMarketplaceSellerFullAccess	2195
使用此策略	2195
策略详细信息	2195
策略版本	2195
JSON 策略文档	2195
了解更多信息	2199
AWSMarketplaceSellerProductsFullAccess	2199
使用此策略	2199
策略详细信息	2199
策略版本	2199
JSON 策略文档	2200
了解更多信息	2201
AWSMarketplaceSellerProductsReadOnly	2202
使用此策略	2202
策略详细信息	2202
策略版本	2202
JSON 策略文档	2202
了解更多信息	2203
AWSMediaConnectServicePolicy	2203
使用此策略	2203
策略详细信息	2203
策略版本	2204
JSON 策略文档	2204
了解更多信息	2205
AWSMediaTailorServiceRolePolicy	2205
使用此策略	2205
策略详细信息	2205
策略版本	2206
JSON 策略文档	2206
了解更多信息	2206

AWSMigrationHubDiscoveryAccess	2207
使用此策略	2207
策略详细信息	2207
策略版本	2207
JSON 策略文档	2207
了解更多信息	2208
AWSMigrationHubDMSAccess	2209
使用此策略	2209
策略详细信息	2209
策略版本	2209
JSON 策略文档	2209
了解更多信息	2210
AWSMigrationHubFullAccess	2210
使用此策略	2211
策略详细信息	2211
策略版本	2211
JSON 策略文档	2211
了解更多信息	2212
AWSMigrationHubOrchestratorConsoleFullAccess	2213
使用此策略	2213
策略详细信息	2213
策略版本	2213
JSON 策略文档	2213
了解更多信息	2216
AWSMigrationHubOrchestratorInstanceRolePolicy	2217
使用此策略	2217
策略详细信息	2217
策略版本	2217
JSON 策略文档	2217
了解更多信息	2218
AWSMigrationHubOrchestratorPlugin	2218
使用此策略	2218
策略详细信息	2218
策略版本	2219
JSON 策略文档	2219
了解更多信息	2220

AWSMigrationHubOrchestratorServiceRolePolicy	2220
使用此策略	2220
策略详细信息	2220
策略版本	2221
JSON 策略文档	2221
了解更多信息	2224
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	2225
使用此策略	2225
策略详细信息	2225
策略版本	2225
JSON 策略文档	2225
了解更多信息	2231
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	2231
使用此策略	2231
策略详细信息	2231
策略版本	2232
JSON 策略文档	2232
了解更多信息	2233
AWSMigrationHubRefactorSpacesFullAccess	2233
使用此策略	2234
策略详细信息	2234
策略版本	2234
JSON 策略文档	2234
了解更多信息	2240
AWSMigrationHubRefactorSpacesServiceRolePolicy	2241
使用此策略	2241
策略详细信息	2241
策略版本	2241
JSON 策略文档	2241
了解更多信息	2245
AWSMigrationHubSMSAccess	2245
使用此策略	2245
策略详细信息	2245
策略版本	2246
JSON 策略文档	2246
了解更多信息	2247

AWSMigrationHubStrategyCollector	2247
使用此策略	2247
策略详细信息	2247
策略版本	2247
JSON 策略文档	2248
了解更多信息	2250
AWSMigrationHubStrategyConsoleFullAccess	2250
使用此策略	2250
策略详细信息	2250
策略版本	2251
JSON 策略文档	2251
了解更多信息	2252
AWSMigrationHubStrategyServiceRolePolicy	2253
使用此策略	2253
策略详细信息	2253
策略版本	2253
JSON 策略文档	2253
了解更多信息	2254
AWSMobileHub_FullAccess	2254
使用此策略	2254
策略详细信息	2255
策略版本	2255
JSON 策略文档	2255
了解更多信息	2256
AWSMobileHub_ReadOnly	2257
使用此策略	2257
策略详细信息	2257
策略版本	2257
JSON 策略文档	2257
了解更多信息	2258
AWSMSKReplicatorExecutionRole	2259
使用此策略	2259
策略详细信息	2259
策略版本	2259
JSON 策略文档	2259
了解更多信息	2261

AWSNetworkFirewallServiceRolePolicy	2261
使用此策略	2261
策略详细信息	2261
策略版本	2261
JSON 策略文档	2261
了解更多信息	2263
AWSNetworkManagerCloudWANServiceRolePolicy	2263
使用此策略	2263
策略详细信息	2263
策略版本	2264
JSON 策略文档	2264
了解更多信息	2264
AWSNetworkManagerFullAccess	2264
使用此策略	2264
策略详细信息	2265
策略版本	2265
JSON 策略文档	2265
了解更多信息	2266
AWSNetworkManagerReadOnlyAccess	2266
使用此策略	2266
策略详细信息	2266
策略版本	2266
JSON 策略文档	2266
了解更多信息	2267
AWSNetworkManagerServiceRolePolicy	2267
使用此策略	2267
策略详细信息	2267
策略版本	2268
JSON 策略文档	2268
了解更多信息	2269
AWSOpsWorks_FullAccess	2269
使用此策略	2269
策略详细信息	2269
策略版本	2269
JSON 策略文档	2269
了解更多信息	2270

AWSOpsWorksCloudWatchLogs	2271
使用此策略	2271
策略详细信息	2271
策略版本	2271
JSON 策略文档	2271
了解更多信息	2272
AWSOpsWorksCMInstanceProfileRole	2272
使用此策略	2272
策略详细信息	2272
策略版本	2272
JSON 策略文档	2273
了解更多信息	2274
AWSOpsWorksCMServiceRole	2274
使用此策略	2274
策略详细信息	2274
策略版本	2274
JSON 策略文档	2274
了解更多信息	2278
AWSOpsWorksInstanceRegistration	2279
使用此策略	2279
策略详细信息	2279
策略版本	2279
JSON 策略文档	2279
了解更多信息	2280
AWSOpsWorksRegisterCLI_EC2	2280
使用此策略	2280
策略详细信息	2280
策略版本	2280
JSON 策略文档	2281
了解更多信息	2281
AWSOpsWorksRegisterCLI_OnPremises	2282
使用此策略	2282
策略详细信息	2282
策略版本	2282
JSON 策略文档	2282
了解更多信息	2284

AWSOrganizationsFullAccess	2284
使用此策略	2284
策略详细信息	2284
策略版本	2284
JSON 策略文档	2285
了解更多信息	2286
AWSOrganizationsReadOnlyAccess	2286
使用此策略	2286
策略详细信息	2286
策略版本	2286
JSON 策略文档	2286
了解更多信息	2287
AWSOrganizationsServiceTrustPolicy	2287
使用此策略	2287
策略详细信息	2288
策略版本	2288
JSON 策略文档	2288
了解更多信息	2289
AWSOutpostsAuthorizeServerPolicy	2289
使用此策略	2289
策略详细信息	2289
策略版本	2289
JSON 策略文档	2289
了解更多信息	2290
AWSOutpostsServiceRolePolicy	2290
使用此策略	2290
策略详细信息	2290
策略版本	2290
JSON 策略文档	2291
了解更多信息	2291
AWSPanoramaApplianceRolePolicy	2291
使用此策略	2291
策略详细信息	2291
策略版本	2292
JSON 策略文档	2292
了解更多信息	2292

AWSPanoramaApplianceServiceRolePolicy	2293
使用此策略	2293
策略详细信息	2293
策略版本	2293
JSON 策略文档	2293
了解更多信息	2295
AWSPanoramaFullAccess	2295
使用此策略	2295
策略详细信息	2295
策略版本	2295
JSON 策略文档	2295
了解更多信息	2298
AWSPanoramaGreengrassGroupRolePolicy	2298
使用此策略	2298
策略详细信息	2298
策略版本	2299
JSON 策略文档	2299
了解更多信息	2300
AWSPanoramaSageMakerRolePolicy	2300
使用此策略	2300
策略详细信息	2300
策略版本	2301
JSON 策略文档	2301
了解更多信息	2301
AWSPanoramaServiceLinkedRolePolicy	2302
使用此策略	2302
策略详细信息	2302
策略版本	2302
JSON 策略文档	2302
了解更多信息	2305
AWSPanoramaServiceRolePolicy	2305
使用此策略	2305
策略详细信息	2305
策略版本	2305
JSON 策略文档	2306
了解更多信息	2313

AWSPriceListServiceFullAccess	2313
使用此策略	2313
策略详细信息	2313
策略版本	2313
JSON 策略文档	2313
了解更多信息	2314
AWSPrivateCAAuditor	2314
使用此策略	2314
策略详细信息	2314
策略版本	2314
JSON 策略文档	2315
了解更多信息	2315
AWSPrivateCAFullAccess	2315
使用此策略	2316
策略详细信息	2316
策略版本	2316
JSON 策略文档	2316
了解更多信息	2316
AWSPrivateCAPrivilegedUser	2317
使用此策略	2317
策略详细信息	2317
策略版本	2317
JSON 策略文档	2317
了解更多信息	2318
AWSPrivateCAReadOnly	2319
使用此策略	2319
策略详细信息	2319
策略版本	2319
JSON 策略文档	2319
了解更多信息	2320
AWSPrivateCAUser	2320
使用此策略	2320
策略详细信息	2320
策略版本	2320
JSON 策略文档	2321
了解更多信息	2322

AWSPRivateMarketplaceAdminFullAccess	2322
使用此策略	2322
策略详细信息	2322
策略版本	2323
JSON 策略文档	2323
了解更多信息	2324
AWSPRivateMarketplaceRequests	2324
使用此策略	2324
策略详细信息	2325
策略版本	2325
JSON 策略文档	2325
了解更多信息	2325
AWSPRivateNetworksServiceRolePolicy	2326
使用此策略	2326
策略详细信息	2326
策略版本	2326
JSON 策略文档	2326
了解更多信息	2327
AWSProtonCodeBuildProvisioningBasicAccess	2327
使用此策略	2327
策略详细信息	2327
策略版本	2327
JSON 策略文档	2327
了解更多信息	2328
AWSProtonCodeBuildProvisioningServiceRolePolicy	2328
使用此策略	2328
策略详细信息	2328
策略版本	2329
JSON 策略文档	2329
了解更多信息	2330
AWSProtonDeveloperAccess	2330
使用此策略	2330
策略详细信息	2331
策略版本	2331
JSON 策略文档	2331
了解更多信息	2333

AWSProtonFullAccess	2333
使用此策略	2334
策略详细信息	2334
策略版本	2334
JSON 策略文档	2334
了解更多信息	2336
AWSProtonReadOnlyAccess	2336
使用此策略	2336
策略详细信息	2337
策略版本	2337
JSON 策略文档	2337
了解更多信息	2338
AWSProtonServiceGitSyncServiceRolePolicy	2339
使用此策略	2339
策略详细信息	2339
策略版本	2339
JSON 策略文档	2339
了解更多信息	2340
AWSProtonSyncServiceRolePolicy	2340
使用此策略	2340
策略详细信息	2340
策略版本	2341
JSON 策略文档	2341
了解更多信息	2342
AWSPurchaseOrdersServiceRolePolicy	2342
使用此策略	2342
策略详细信息	2342
策略版本	2342
JSON 策略文档	2343
了解更多信息	2343
AWSQuickSightAssetBundleExportPolicy	2344
使用此策略	2344
策略详细信息	2344
策略版本	2344
JSON 策略文档	2344
了解更多信息	2346

AWSQuickSightAssetBundleImportPolicy	2346
使用此策略	2347
策略详细信息	2347
策略版本	2347
JSON 策略文档	2347
了解更多信息	2350
AWSQuickSightAthenaAccess	2350
使用此策略	2350
策略详细信息	2350
策略版本	2351
JSON 策略文档	2351
了解更多信息	2353
AWSQuickSightDescribeRDS	2353
使用此策略	2353
策略详细信息	2353
策略版本	2354
JSON 策略文档	2354
了解更多信息	2354
AWSQuickSightDescribeRedshift	2354
使用此策略	2354
策略详细信息	2355
策略版本	2355
JSON 策略文档	2355
了解更多信息	2355
AWSQuickSightElasticsearchPolicy	2356
使用此策略	2356
策略详细信息	2356
策略版本	2356
JSON 策略文档	2356
了解更多信息	2357
AWSQuickSightIoTAnalyticsAccess	2357
使用此策略	2358
策略详细信息	2358
策略版本	2358
JSON 策略文档	2358
了解更多信息	2358

AWSQuickSightListIAM	2359
使用此策略	2359
策略详细信息	2359
策略版本	2359
JSON 策略文档	2359
了解更多信息	2360
AWSQuicksightOpenSearchPolicy	2360
使用此策略	2360
策略详细信息	2360
策略版本	2360
JSON 策略文档	2361
了解更多信息	2362
AWSQuickSightSageMakerPolicy	2362
使用此策略	2362
策略详细信息	2362
策略版本	2362
JSON 策略文档	2362
了解更多信息	2364
AWSQuickSightTimestreamPolicy	2364
使用此策略	2364
策略详细信息	2364
策略版本	2364
JSON 策略文档	2364
了解更多信息	2365
AWSReachabilityAnalyzerServiceRolePolicy	2365
使用此策略	2365
策略详细信息	2365
策略版本	2366
JSON 策略文档	2366
了解更多信息	2368
AWSRefactoringToolkitFullAccess	2368
使用此策略	2369
策略详细信息	2369
策略版本	2369
JSON 策略文档	2369
了解更多信息	2382

AWSRefactoringToolkitSidecarPolicy	2383
使用此策略	2383
策略详细信息	2383
策略版本	2383
JSON 策略文档	2383
了解更多信息	2384
AWSrePostPrivateCloudWatchAccess	2384
使用此策略	2385
策略详细信息	2385
策略版本	2385
JSON 策略文档	2385
了解更多信息	2386
AWSRepostSpaceSupportOperationsPolicy	2386
使用此策略	2386
策略详细信息	2386
策略版本	2386
JSON 策略文档	2386
了解更多信息	2387
AWSResilienceHubAssessmentExecutionPolicy	2387
使用此策略	2387
策略详细信息	2387
策略版本	2388
JSON 策略文档	2388
了解更多信息	2392
AWSResourceAccessManagerFullAccess	2392
使用此策略	2392
策略详细信息	2392
策略版本	2393
JSON 策略文档	2393
了解更多信息	2393
AWSResourceAccessManagerReadOnlyAccess	2393
使用此策略	2393
策略详细信息	2394
策略版本	2394
JSON 策略文档	2394
了解更多信息	2394

AWSResourceAccessManagerResourceShareParticipantAccess	2395
使用此策略	2395
策略详细信息	2395
策略版本	2395
JSON 策略文档	2395
了解更多信息	2396
AWSResourceAccessManagerServiceRolePolicy	2396
使用此策略	2396
策略详细信息	2396
策略版本	2396
JSON 策略文档	2397
了解更多信息	2397
AWSResourceExplorerFullAccess	2398
使用此策略	2398
策略详细信息	2398
策略版本	2398
JSON 策略文档	2398
了解更多信息	2399
AWSResourceExplorerOrganizationsAccess	2399
使用此策略	2399
策略详细信息	2399
策略版本	2400
JSON 策略文档	2400
了解更多信息	2401
AWSResourceExplorerReadOnlyAccess	2402
使用此策略	2402
策略详细信息	2402
策略版本	2402
JSON 策略文档	2402
了解更多信息	2403
AWSResourceExplorerServiceRolePolicy	2403
使用此策略	2403
策略详细信息	2403
策略版本	2404
JSON 策略文档	2404
了解更多信息	2413

AWSResourceGroupsReadOnlyAccess	2413
使用此策略	2413
策略详细信息	2413
策略版本	2413
JSON 策略文档	2414
了解更多信息	2415
AWSRoboMaker_FullAccess	2415
使用此策略	2415
策略详细信息	2415
策略版本	2416
JSON 策略文档	2416
了解更多信息	2417
AWSRoboMakerReadOnlyAccess	2417
使用此策略	2417
策略详细信息	2417
策略版本	2418
JSON 策略文档	2418
了解更多信息	2418
AWSRoboMakerServicePolicy	2418
使用此策略	2419
策略详细信息	2419
策略版本	2419
JSON 策略文档	2419
了解更多信息	2421
AWSRoboMakerServiceRolePolicy	2421
使用此策略	2421
策略详细信息	2421
策略版本	2421
JSON 策略文档	2421
了解更多信息	2423
AWSRolesAnywhereServicePolicy	2423
使用此策略	2423
策略详细信息	2423
策略版本	2423
JSON 策略文档	2423
了解更多信息	2424

AWSS3OnOutpostsServiceRolePolicy	2424
使用此策略	2424
策略详细信息	2425
策略版本	2425
JSON 策略文档	2425
了解更多信息	2428
AWSSavingsPlansFullAccess	2428
使用此策略	2428
策略详细信息	2428
策略版本	2428
JSON 策略文档	2428
了解更多信息	2429
AWSSavingsPlansReadOnlyAccess	2429
使用此策略	2429
策略详细信息	2429
策略版本	2429
JSON 策略文档	2430
了解更多信息	2430
AWSSecurityHubFullAccess	2430
使用此策略	2430
策略详细信息	2430
策略版本	2431
JSON 策略文档	2431
了解更多信息	2432
AWSSecurityHubOrganizationsAccess	2432
使用此策略	2432
策略详细信息	2432
策略版本	2432
JSON 策略文档	2433
了解更多信息	2434
AWSSecurityHubReadOnlyAccess	2434
使用此策略	2434
策略详细信息	2434
策略版本	2434
JSON 策略文档	2435
了解更多信息	2435

AWSSecurityHubServiceRolePolicy	2435
使用此策略	2435
策略详细信息	2435
策略版本	2436
JSON 策略文档	2436
了解更多信息	2438
AWSServiceCatalogAdminFullAccess	2438
使用此策略	2438
策略详细信息	2438
策略版本	2438
JSON 策略文档	2439
了解更多信息	2441
AWSServiceCatalogAdminReadOnlyAccess	2442
使用此策略	2442
策略详细信息	2442
策略版本	2442
JSON 策略文档	2442
了解更多信息	2443
AWSServiceCatalogAppRegistryFullAccess	2444
使用此策略	2444
策略详细信息	2444
策略版本	2444
JSON 策略文档	2444
了解更多信息	2446
AWSServiceCatalogAppRegistryReadOnlyAccess	2447
使用此策略	2447
策略详细信息	2447
策略版本	2447
JSON 策略文档	2447
了解更多信息	2448
AWSServiceCatalogAppRegistryServiceRolePolicy	2448
使用此策略	2448
策略详细信息	2448
策略版本	2449
JSON 策略文档	2449
了解更多信息	2450

AWSServiceCatalogEndUserFullAccess	2450
使用此策略	2450
策略详细信息	2450
策略版本	2451
JSON 策略文档	2451
了解更多信息	2453
AWSServiceCatalogEndUserReadOnlyAccess	2453
使用此策略	2453
策略详细信息	2453
策略版本	2453
JSON 策略文档	2454
了解更多信息	2455
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	2455
使用此策略	2456
策略详细信息	2456
策略版本	2456
JSON 策略文档	2456
了解更多信息	2457
AWSServiceCatalogSyncServiceRolePolicy	2457
使用此策略	2457
策略详细信息	2457
策略版本	2457
JSON 策略文档	2457
了解更多信息	2458
AWSServiceRoleForAmazonEKSNodegroup	2459
使用此策略	2459
策略详细信息	2459
策略版本	2459
JSON 策略文档	2459
了解更多信息	2463
AWSServiceRoleForAmazonQDeveloper	2463
使用此策略	2464
策略详细信息	2464
策略版本	2464
JSON 策略文档	2464
了解更多信息	2465

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy	2465
使用此策略	2465
策略详细信息	2465
策略版本	2465
JSON 策略文档	2465
了解更多信息	2466
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy	2466
使用此策略	2466
策略详细信息	2466
策略版本	2466
JSON 策略文档	2467
了解更多信息	2467
AWSServiceRoleForCodeGuru-Profiler	2467
使用此策略	2467
策略详细信息	2468
策略版本	2468
JSON 策略文档	2468
了解更多信息	2468
AWSServiceRoleForCodeWhispererPolicy	2469
使用此策略	2469
策略详细信息	2469
策略版本	2469
JSON 策略文档	2469
了解更多信息	2471
AWSServiceRoleForEC2ScheduledInstances	2471
使用此策略	2471
策略详细信息	2471
策略版本	2472
JSON 策略文档	2472
了解更多信息	2473
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	2473
使用此策略	2473
策略详细信息	2473
策略版本	2473
JSON 策略文档	2473
了解更多信息	2474

AWSServiceRoleForImageBuilder	2474
使用此策略	2474
策略详细信息	2474
策略版本	2474
JSON 策略文档	2475
了解更多信息	2484
AWSServiceRoleForIoTSiteWise	2484
使用此策略	2484
策略详细信息	2485
策略版本	2485
JSON 策略文档	2485
了解更多信息	2486
AWSServiceRoleForLogDeliveryPolicy	2486
使用此策略	2487
策略详细信息	2487
策略版本	2487
JSON 策略文档	2487
了解更多信息	2488
AWSServiceRoleForMonitronPolicy	2488
使用此策略	2488
策略详细信息	2488
策略版本	2488
JSON 策略文档	2488
了解更多信息	2489
AWSServiceRoleForNeptuneGraphPolicy	2489
使用此策略	2489
策略详细信息	2489
策略版本	2490
JSON 策略文档	2490
了解更多信息	2491
AWSServiceRoleForPrivateMarketplaceAdminPolicy	2491
使用此策略	2491
策略详细信息	2491
策略版本	2492
JSON 策略文档	2492
了解更多信息	2493

AWSServiceRoleForSMS	2494
使用此策略	2494
策略详细信息	2494
策略版本	2494
JSON 策略文档	2494
了解更多信息	2501
AWSServiceRoleForUserSubscriptions	2501
使用此策略	2501
策略详细信息	2501
策略版本	2501
JSON 策略文档	2502
了解更多信息	2502
AWSServiceRolePolicyForBackupReports	2502
使用此策略	2503
策略详细信息	2503
策略版本	2503
JSON 策略文档	2503
了解更多信息	2504
AWSServiceRolePolicyForBackupRestoreTesting	2504
使用此策略	2505
策略详细信息	2505
策略版本	2505
JSON 策略文档	2505
了解更多信息	2508
AWSShieldDRTAcessPolicy	2508
使用此策略	2508
策略详细信息	2508
策略版本	2508
JSON 策略文档	2509
了解更多信息	2510
AWSShieldServiceRolePolicy	2510
使用此策略	2510
策略详细信息	2510
策略版本	2510
JSON 策略文档	2510
了解更多信息	2511

AWSSSMForSAPServiceLinkedRolePolicy	2511
使用此策略	2511
策略详细信息	2511
策略版本	2512
JSON 策略文档	2512
了解更多信息	2518
AWSSSMOpsInsightsServiceRolePolicy	2518
使用此策略	2518
策略详细信息	2519
策略版本	2519
JSON 策略文档	2519
了解更多信息	2520
AWSSSODirectoryAdministrator	2520
使用此策略	2520
策略详细信息	2520
策略版本	2520
JSON 策略文档	2520
了解更多信息	2521
AWSSSODirectoryReadOnly	2521
使用此策略	2521
策略详细信息	2521
策略版本	2522
JSON 策略文档	2522
了解更多信息	2522
AWSSSOMasterAccountAdministrator	2522
使用此策略	2523
策略详细信息	2523
策略版本	2523
JSON 策略文档	2523
了解更多信息	2525
AWSSSOMemberAccountAdministrator	2525
使用此策略	2525
策略详细信息	2525
策略版本	2525
JSON 策略文档	2526
了解更多信息	2527

AWSSSOReadOnly	2527
使用此策略	2527
策略详细信息	2527
策略版本	2528
JSON 策略文档	2528
了解更多信息	2529
AWSSSOServiceRolePolicy	2529
使用此策略	2529
策略详细信息	2529
策略版本	2529
JSON 策略文档	2529
了解更多信息	2533
AWSSStepFunctionsConsoleFullAccess	2533
使用此策略	2533
策略详细信息	2533
策略版本	2534
JSON 策略文档	2534
了解更多信息	2534
AWSSStepFunctionsFullAccess	2535
使用此策略	2535
策略详细信息	2535
策略版本	2535
JSON 策略文档	2535
了解更多信息	2536
AWSSStepFunctionsReadOnlyAccess	2536
使用此策略	2536
策略详细信息	2536
策略版本	2536
JSON 策略文档	2536
了解更多信息	2537
AWSSStorageGatewayFullAccess	2537
使用此策略	2537
策略详细信息	2538
策略版本	2538
JSON 策略文档	2538
了解更多信息	2539

AWSSStorageGatewayReadOnlyAccess	2539
使用此策略	2539
策略详细信息	2539
策略版本	2539
JSON 策略文档	2539
了解更多信息	2540
AWSSStorageGatewayServiceRolePolicy	2540
使用此策略	2540
策略详细信息	2541
策略版本	2541
JSON 策略文档	2541
了解更多信息	2541
AWSSupplyChainFederationAdminAccess	2542
使用此策略	2542
策略详细信息	2542
策略版本	2542
JSON 策略文档	2542
了解更多信息	2548
AWSSupportAccess	2548
使用此策略	2548
策略详细信息	2548
策略版本	2548
JSON 策略文档	2548
了解更多信息	2549
AWSSupportAppFullAccess	2549
使用此策略	2549
策略详细信息	2549
策略版本	2549
JSON 策略文档	2550
了解更多信息	2550
AWSSupportAppReadOnlyAccess	2551
使用此策略	2551
策略详细信息	2551
策略版本	2551
JSON 策略文档	2551
了解更多信息	2552

AWSSupportPlansFullAccess	2552
使用此策略	2552
策略详细信息	2552
策略版本	2552
JSON 策略文档	2552
了解更多信息	2553
AWSSupportPlansReadOnlyAccess	2553
使用此策略	2553
策略详细信息	2553
策略版本	2554
JSON 策略文档	2554
了解更多信息	2554
AWSSupportServiceRolePolicy	2554
使用此策略	2554
策略详细信息	2555
策略版本	2555
JSON 策略文档	2555
了解更多信息	2630
AWSSystemsManagerAccountDiscoveryServicePolicy	2630
使用此策略	2631
策略详细信息	2631
策略版本	2631
JSON 策略文档	2631
了解更多信息	2632
AWSSystemsManagerChangeManagementServicePolicy	2632
使用此策略	2632
策略详细信息	2632
策略版本	2632
JSON 策略文档	2632
了解更多信息	2634
AWSSystemsManagerForSAPFullAccess	2634
使用此策略	2634
策略详细信息	2634
策略版本	2635
JSON 策略文档	2635
了解更多信息	2636

AWSSystemsManagerForSAPReadOnlyAccess	2636
使用此策略	2636
策略详细信息	2636
策略版本	2636
JSON 策略文档	2636
了解更多信息	2637
AWSSystemsManagerOpsDataSyncServiceRolePolicy	2637
使用此策略	2637
策略详细信息	2637
策略版本	2637
JSON 策略文档	2638
了解更多信息	2641
AWSThinkboxAssetServerPolicy	2641
使用此策略	2642
策略详细信息	2642
策略版本	2642
JSON 策略文档	2642
了解更多信息	2643
AWSThinkboxAWSPortalAdminPolicy	2643
使用此策略	2643
策略详细信息	2643
策略版本	2643
JSON 策略文档	2644
了解更多信息	2653
AWSThinkboxAWSPortalGatewayPolicy	2654
使用此策略	2654
策略详细信息	2654
策略版本	2654
JSON 策略文档	2654
了解更多信息	2656
AWSThinkboxAWSPortalWorkerPolicy	2656
使用此策略	2656
策略详细信息	2656
策略版本	2657
JSON 策略文档	2657
了解更多信息	2659

AWSThinkboxDeadlineResourceTrackerAccessPolicy	2659
使用此策略	2659
策略详细信息	2659
策略版本	2659
JSON 策略文档	2660
了解更多信息	2662
AWSThinkboxDeadlineResourceTrackerAdminPolicy	2662
使用此策略	2663
策略详细信息	2663
策略版本	2663
JSON 策略文档	2663
了解更多信息	2669
AWSThinkboxDeadlineSpotEventPluginAdminPolicy	2669
使用此策略	2669
策略详细信息	2669
策略版本	2670
JSON 策略文档	2670
了解更多信息	2672
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	2673
使用此策略	2673
策略详细信息	2673
策略版本	2673
JSON 策略文档	2673
了解更多信息	2675
AWSTransferConsoleFullAccess	2675
使用此策略	2675
策略详细信息	2675
策略版本	2675
JSON 策略文档	2675
了解更多信息	2676
AWSTransferFullAccess	2677
使用此策略	2677
策略详细信息	2677
策略版本	2677
JSON 策略文档	2677
了解更多信息	2678

AWSTransferLoggingAccess	2678
使用此策略	2678
策略详细信息	2678
策略版本	2679
JSON 策略文档	2679
了解更多信息	2679
AWSTransferReadOnlyAccess	2679
使用此策略	2680
策略详细信息	2680
策略版本	2680
JSON 策略文档	2680
了解更多信息	2681
AWSTrustedAdvisorPriorityFullAccess	2681
使用此策略	2681
策略详细信息	2681
策略版本	2681
JSON 策略文档	2681
了解更多信息	2683
AWSTrustedAdvisorPriorityReadOnlyAccess	2683
使用此策略	2683
策略详细信息	2684
策略版本	2684
JSON 策略文档	2684
了解更多信息	2685
AWSTrustedAdvisorReportingServiceRolePolicy	2685
使用此策略	2685
策略详细信息	2685
策略版本	2686
JSON 策略文档	2686
了解更多信息	2686
AWSTrustedAdvisorServiceRolePolicy	2686
使用此策略	2687
策略详细信息	2687
策略版本	2687
JSON 策略文档	2687
了解更多信息	2690

AWSUserNotificationsServiceLinkedRolePolicy	2690
使用此策略	2690
策略详细信息	2690
策略版本	2691
JSON 策略文档	2691
了解更多信息	2691
AWSVendorInsightsAssessorFullAccess	2692
使用此策略	2692
策略详细信息	2692
策略版本	2692
JSON 策略文档	2692
了解更多信息	2693
AWSVendorInsightsAssessorReadOnly	2694
使用此策略	2694
策略详细信息	2694
策略版本	2694
JSON 策略文档	2694
了解更多信息	2695
AWSVendorInsightsVendorFullAccess	2695
使用此策略	2695
策略详细信息	2695
策略版本	2695
JSON 策略文档	2696
了解更多信息	2697
AWSVendorInsightsVendorReadOnly	2697
使用此策略	2698
策略详细信息	2698
策略版本	2698
JSON 策略文档	2698
了解更多信息	2699
AWSVpcLatticeServiceRolePolicy	2699
使用此策略	2699
策略详细信息	2699
策略版本	2700
JSON 策略文档	2700
了解更多信息	2700

AWSVPCS2SVpnServiceRolePolicy	2700
使用此策略	2701
策略详细信息	2701
策略版本	2701
JSON 策略文档	2701
了解更多信息	2702
AWSVPCTransitGatewayServiceRolePolicy	2702
使用此策略	2702
策略详细信息	2702
策略版本	2702
JSON 策略文档	2702
了解更多信息	2703
AWSVPCVerifiedAccessServiceRolePolicy	2703
使用此策略	2703
策略详细信息	2703
策略版本	2704
JSON 策略文档	2704
了解更多信息	2705
AWSWAFConsoleFullAccess	2705
使用此策略	2706
策略详细信息	2706
策略版本	2706
JSON 策略文档	2706
了解更多信息	2708
AWSWAFConsoleReadOnlyAccess	2708
使用此策略	2709
策略详细信息	2709
策略版本	2709
JSON 策略文档	2709
了解更多信息	2710
AWSWAFFullAccess	2710
使用此策略	2710
策略详细信息	2710
策略版本	2711
JSON 策略文档	2711
了解更多信息	2712

AWSWAFReadOnlyAccess	2713
使用此策略	2713
策略详细信息	2713
策略版本	2713
JSON 策略文档	2713
了解更多信息	2714
AWSWellArchitectedDiscoveryServiceRolePolicy	2714
使用此策略	2714
策略详细信息	2714
策略版本	2715
JSON 策略文档	2715
了解更多信息	2716
AWSWellArchitectedOrganizationsServiceRolePolicy	2716
使用此策略	2717
策略详细信息	2717
策略版本	2717
JSON 策略文档	2717
了解更多信息	2718
AWSWickrFullAccess	2718
使用此策略	2718
策略详细信息	2718
策略版本	2718
JSON 策略文档	2718
了解更多信息	2719
AWSXrayCrossAccountSharingConfiguration	2719
使用此策略	2719
策略详细信息	2719
策略版本	2719
JSON 策略文档	2720
了解更多信息	2720
AWSXRayDaemonWriteAccess	2721
使用此策略	2721
策略详细信息	2721
策略版本	2721
JSON 策略文档	2721
了解更多信息	2722

AWSXrayFullAccess	2722
使用此策略	2722
策略详细信息	2722
策略版本	2723
JSON 策略文档	2723
了解更多信息	2723
AWSXrayReadOnlyAccess	2723
使用此策略	2724
策略详细信息	2724
策略版本	2724
JSON 策略文档	2724
了解更多信息	2725
AWSXrayWriteOnlyAccess	2725
使用此策略	2725
策略详细信息	2725
策略版本	2726
JSON 策略文档	2726
了解更多信息	2726
AWSZonalAutoshiftPracticeRunSLRPolicy	2726
使用此策略	2727
策略详细信息	2727
策略版本	2727
JSON 策略文档	2727
了解更多信息	2728
BatchServiceRolePolicy	2728
使用此策略	2728
策略详细信息	2728
策略版本	2728
JSON 策略文档	2729
了解更多信息	2735
Billing	2735
使用此策略	2735
策略详细信息	2735
策略版本	2735
JSON 策略文档	2735
了解更多信息	2738

CertificateManagerServiceRolePolicy	2738
使用此策略	2739
策略详细信息	2739
策略版本	2739
JSON 策略文档	2739
了解更多信息	2739
ClientVPNServiceConnectionsRolePolicy	2740
使用此策略	2740
策略详细信息	2740
策略版本	2740
JSON 策略文档	2740
了解更多信息	2741
ClientVPNServiceRolePolicy	2741
使用此策略	2741
策略详细信息	2741
策略版本	2741
JSON 策略文档	2741
了解更多信息	2742
CloudFormationStackSetsOrgAdminServiceRolePolicy	2742
使用此策略	2743
策略详细信息	2743
策略版本	2743
JSON 策略文档	2743
了解更多信息	2744
CloudFormationStackSetsOrgMemberServiceRolePolicy	2744
使用此策略	2744
策略详细信息	2744
策略版本	2744
JSON 策略文档	2744
了解更多信息	2745
CloudFrontFullAccess	2745
使用此策略	2746
策略详细信息	2746
策略版本	2746
JSON 策略文档	2746
了解更多信息	2747

CloudFrontReadOnlyAccess	2747
使用此策略	2748
策略详细信息	2748
策略版本	2748
JSON 策略文档	2748
了解更多信息	2749
CloudHSMServiceRolePolicy	2749
使用此策略	2749
策略详细信息	2749
策略版本	2749
JSON 策略文档	2750
了解更多信息	2750
CloudSearchFullAccess	2750
使用此策略	2750
策略详细信息	2750
策略版本	2751
JSON 策略文档	2751
了解更多信息	2751
CloudSearchReadOnlyAccess	2751
使用此策略	2752
策略详细信息	2752
策略版本	2752
JSON 策略文档	2752
了解更多信息	2752
CloudTrailServiceRolePolicy	2753
使用此策略	2753
策略详细信息	2753
策略版本	2753
JSON 策略文档	2753
了解更多信息	2755
CloudWatch-CrossAccountAccess	2755
使用此策略	2755
策略详细信息	2755
策略版本	2755
JSON 策略文档	2756
了解更多信息	2756

CloudWatchActionsEC2Access	2756
使用此策略	2756
策略详细信息	2756
策略版本	2757
JSON 策略文档	2757
了解更多信息	2757
CloudWatchAgentAdminPolicy	2758
使用此策略	2758
策略详细信息	2758
策略版本	2758
JSON 策略文档	2758
了解更多信息	2759
CloudWatchAgentServerPolicy	2759
使用此策略	2759
策略详细信息	2760
策略版本	2760
JSON 策略文档	2760
了解更多信息	2761
CloudWatchApplicationInsightsFullAccess	2761
使用此策略	2761
策略详细信息	2761
策略版本	2761
JSON 策略文档	2762
了解更多信息	2763
CloudWatchApplicationInsightsReadOnlyAccess	2763
使用此策略	2763
策略详细信息	2763
策略版本	2764
JSON 策略文档	2764
了解更多信息	2764
CloudwatchApplicationInsightsServiceLinkedRolePolicy	2764
使用此策略	2765
策略详细信息	2765
策略版本	2765
JSON 策略文档	2765
了解更多信息	2775

CloudWatchApplicationSignalsFullAccess	2775
使用此策略	2775
策略详细信息	2775
策略版本	2775
JSON 策略文档	2776
了解更多信息	2778
CloudWatchApplicationSignalsReadOnlyAccess	2779
使用此策略	2779
策略详细信息	2779
策略版本	2779
JSON 策略文档	2779
了解更多信息	2781
CloudWatchApplicationSignalsServiceRolePolicy	2782
使用此策略	2782
策略详细信息	2782
策略版本	2782
JSON 策略文档	2782
了解更多信息	2784
CloudWatchAutomaticDashboardsAccess	2785
使用此策略	2785
策略详细信息	2785
策略版本	2785
JSON 策略文档	2785
了解更多信息	2787
CloudWatchCrossAccountSharingConfiguration	2787
使用此策略	2787
策略详细信息	2787
策略版本	2787
JSON 策略文档	2787
了解更多信息	2788
CloudWatchEventsBuiltInTargetExecutionAccess	2788
使用此策略	2789
策略详细信息	2789
策略版本	2789
JSON 策略文档	2789
了解更多信息	2790

CloudWatchEventsFullAccess	2790
使用此策略	2790
策略详细信息	2790
策略版本	2790
JSON 策略文档	2790
了解更多信息	2792
CloudWatchEventsInvocationAccess	2793
使用此策略	2793
策略详细信息	2793
策略版本	2793
JSON 策略文档	2793
了解更多信息	2794
CloudWatchEventsReadOnlyAccess	2794
使用此策略	2794
策略详细信息	2794
策略版本	2794
JSON 策略文档	2794
了解更多信息	2796
CloudWatchEventsServiceRolePolicy	2796
使用此策略	2796
策略详细信息	2796
策略版本	2796
JSON 策略文档	2797
了解更多信息	2797
CloudWatchFullAccess	2797
使用此策略	2797
策略详细信息	2798
策略版本	2798
JSON 策略文档	2798
了解更多信息	2799
CloudWatchFullAccessV2	2799
使用此策略	2799
策略详细信息	2799
策略版本	2800
JSON 策略文档	2800
了解更多信息	2801

CloudWatchInternetMonitorServiceRolePolicy	2801
使用此策略	2802
策略详细信息	2802
策略版本	2802
JSON 策略文档	2802
了解更多信息	2803
CloudWatchLambdaInsightsExecutionRolePolicy	2803
使用此策略	2803
策略详细信息	2803
策略版本	2804
JSON 策略文档	2804
了解更多信息	2804
CloudWatchLogsCrossAccountSharingConfiguration	2805
使用此策略	2805
策略详细信息	2805
策略版本	2805
JSON 策略文档	2805
了解更多信息	2806
CloudWatchLogsFullAccess	2806
使用此策略	2806
策略详细信息	2807
策略版本	2807
JSON 策略文档	2807
了解更多信息	2807
CloudWatchLogsReadOnlyAccess	2808
使用此策略	2808
策略详细信息	2808
策略版本	2808
JSON 策略文档	2808
了解更多信息	2809
CloudWatchNetworkMonitorServiceRolePolicy	2809
使用此策略	2809
策略详细信息	2809
策略版本	2809
JSON 策略文档	2810
了解更多信息	2811

CloudWatchReadOnlyAccess	2811
使用此策略	2811
策略详细信息	2811
策略版本	2811
JSON 策略文档	2812
了解更多信息	2813
CloudWatchSyntheticsFullAccess	2813
使用此策略	2813
策略详细信息	2813
策略版本	2814
JSON 策略文档	2814
了解更多信息	2818
CloudWatchSyntheticsReadOnlyAccess	2819
使用此策略	2819
策略详细信息	2819
策略版本	2819
JSON 策略文档	2819
了解更多信息	2820
ComprehendDataAccessRolePolicy	2820
使用此策略	2820
策略详细信息	2820
策略版本	2820
JSON 策略文档	2820
了解更多信息	2821
ComprehendFullAccess	2821
使用此策略	2821
策略详细信息	2821
策略版本	2822
JSON 策略文档	2822
了解更多信息	2822
ComprehendMedicalFullAccess	2822
使用此策略	2823
策略详细信息	2823
策略版本	2823
JSON 策略文档	2823
了解更多信息	2823

ComprehendReadOnly	2824
使用此策略	2824
策略详细信息	2824
策略版本	2824
JSON 策略文档	2824
了解更多信息	2825
ComputeOptimizerReadOnlyAccess	2826
使用此策略	2826
策略详细信息	2826
策略版本	2826
JSON 策略文档	2826
了解更多信息	2827
ComputeOptimizerServiceRolePolicy	2827
使用此策略	2828
策略详细信息	2828
策略版本	2828
JSON 策略文档	2828
了解更多信息	2829
ConfigConformsServiceRolePolicy	2830
使用此策略	2830
策略详细信息	2830
策略版本	2830
JSON 策略文档	2830
了解更多信息	2833
CostOptimizationHubAdminAccess	2833
使用此策略	2833
策略详细信息	2833
策略版本	2834
JSON 策略文档	2834
了解更多信息	2835
CostOptimizationHubReadOnlyAccess	2835
使用此策略	2835
策略详细信息	2835
策略版本	2836
JSON 策略文档	2836
了解更多信息	2836

CostOptimizationHubServiceRolePolicy	2836
使用此策略	2837
策略详细信息	2837
策略版本	2837
JSON 策略文档	2837
了解更多信息	2838
CustomerProfilesServiceLinkedRolePolicy	2838
使用此策略	2838
策略详细信息	2838
策略版本	2838
JSON 策略文档	2839
了解更多信息	2839
DatabaseAdministrator	2839
使用此策略	2840
策略详细信息	2840
策略版本	2840
JSON 策略文档	2840
了解更多信息	2842
DataScientist	2843
使用此策略	2843
策略详细信息	2843
策略版本	2843
JSON 策略文档	2843
了解更多信息	2847
DAXServiceRolePolicy	2847
使用此策略	2847
策略详细信息	2847
策略版本	2848
JSON 策略文档	2848
了解更多信息	2848
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	2848
使用此策略	2849
策略详细信息	2849
策略版本	2849
JSON 策略文档	2849
了解更多信息	2850

DynamoDBKinesisReplicationServiceRolePolicy	2850
使用此策略	2850
策略详细信息	2850
策略版本	2850
JSON 策略文档	2850
了解更多信息	2851
DynamoDBReplicationServiceRolePolicy	2851
使用此策略	2851
策略详细信息	2851
策略版本	2852
JSON 策略文档	2852
了解更多信息	2853
EC2FastLaunchFullAccess	2853
使用此策略	2853
策略详细信息	2853
策略版本	2854
JSON 策略文档	2854
了解更多信息	2856
EC2FastLaunchServiceRolePolicy	2857
使用此策略	2857
策略详细信息	2857
策略版本	2857
JSON 策略文档	2857
了解更多信息	2861
EC2FleetTimeShiftableServiceRolePolicy	2861
使用此策略	2861
策略详细信息	2861
策略版本	2862
JSON 策略文档	2862
了解更多信息	2863
Ec2ImageBuilderCrossAccountDistributionAccess	2863
使用此策略	2864
策略详细信息	2864
策略版本	2864
JSON 策略文档	2864
了解更多信息	2865

EC2ImageBuilderLifecycleExecutionPolicy	2865
使用此策略	2865
策略详细信息	2865
策略版本	2865
JSON 策略文档	2866
了解更多信息	2867
EC2InstanceConnect	2868
使用此策略	2868
策略详细信息	2868
策略版本	2868
JSON 策略文档	2868
了解更多信息	2869
Ec2InstanceConnectEndpoint	2869
使用此策略	2869
策略详细信息	2869
策略版本	2869
JSON 策略文档	2870
了解更多信息	2872
EC2InstanceProfileForImageBuilder	2872
使用此策略	2872
策略详细信息	2872
策略版本	2872
JSON 策略文档	2872
了解更多信息	2873
EC2InstanceProfileForImageBuilderECRContainerBuilds	2874
使用此策略	2874
策略详细信息	2874
策略版本	2874
JSON 策略文档	2874
了解更多信息	2876
ECRReplicationServiceRolePolicy	2876
使用此策略	2876
策略详细信息	2876
策略版本	2876
JSON 策略文档	2876
了解更多信息	2877

ElastiCacheServiceRolePolicy	2877
使用此策略	2877
策略详细信息	2877
策略版本	2877
JSON 策略文档	2878
了解更多信息	2880
ElasticLoadBalancingFullAccess	2880
使用此策略	2880
策略详细信息	2880
策略版本	2880
JSON 策略文档	2880
了解更多信息	2882
ElasticLoadBalancingReadOnly	2882
使用此策略	2882
策略详细信息	2882
策略版本	2882
JSON 策略文档	2883
了解更多信息	2884
ElementalActivationsDownloadSoftwareAccess	2884
使用此策略	2884
策略详细信息	2884
策略版本	2884
JSON 策略文档	2884
了解更多信息	2885
ElementalActivationsFullAccess	2885
使用此策略	2885
策略详细信息	2885
策略版本	2885
JSON 策略文档	2886
了解更多信息	2886
ElementalActivationsGenerateLicenses	2886
使用此策略	2886
策略详细信息	2886
策略版本	2887
JSON 策略文档	2887
了解更多信息	2887

ElementalActivationsReadOnlyAccess	2887
使用此策略	2888
策略详细信息	2888
策略版本	2888
JSON 策略文档	2888
了解更多信息	2888
ElementalAppliancesSoftwareFullAccess	2889
使用此策略	2889
策略详细信息	2889
策略版本	2889
JSON 策略文档	2889
了解更多信息	2890
ElementalAppliancesSoftwareReadOnlyAccess	2890
使用此策略	2890
策略详细信息	2890
策略版本	2890
JSON 策略文档	2891
了解更多信息	2891
ElementalSupportCenterFullAccess	2891
使用此策略	2891
策略详细信息	2891
策略版本	2892
JSON 策略文档	2892
了解更多信息	2892
EMRDescribeClusterPolicyForEMRWAL	2892
使用此策略	2893
策略详细信息	2893
策略版本	2893
JSON 策略文档	2893
了解更多信息	2893
FMSServiceRolePolicy	2894
使用此策略	2894
策略详细信息	2894
策略版本	2894
JSON 策略文档	2894
了解更多信息	2910

FSxDeleteServiceLinkedRoleAccess	2910
使用此策略	2911
策略详细信息	2911
策略版本	2911
JSON 策略文档	2911
了解更多信息	2912
GameLiftGameServerGroupPolicy	2912
使用此策略	2912
策略详细信息	2912
策略版本	2912
JSON 策略文档	2912
了解更多信息	2914
GlobalAcceleratorFullAccess	2914
使用此策略	2914
策略详细信息	2914
策略版本	2915
JSON 策略文档	2915
了解更多信息	2916
GlobalAcceleratorReadOnlyAccess	2916
使用此策略	2916
策略详细信息	2916
策略版本	2916
JSON 策略文档	2917
了解更多信息	2917
GreengrassOTAUpdateArtifactAccess	2917
使用此策略	2917
策略详细信息	2917
策略版本	2918
JSON 策略文档	2918
了解更多信息	2918
GroundTruthSyntheticConsoleFullAccess	2918
使用此策略	2919
策略详细信息	2919
策略版本	2919
JSON 策略文档	2919
了解更多信息	2919

GroundTruthSyntheticConsoleReadOnlyAccess	2920
使用此策略	2920
策略详细信息	2920
策略版本	2920
JSON 策略文档	2920
了解更多信息	2921
Health_OrganizationsServiceRolePolicy	2921
使用此策略	2921
策略详细信息	2921
策略版本	2921
JSON 策略文档	2922
了解更多信息	2922
IAMAccessAdvisorReadOnly	2922
使用此策略	2922
策略详细信息	2923
策略版本	2923
JSON 策略文档	2923
了解更多信息	2924
IAMAccessAnalyzerFullAccess	2924
使用此策略	2924
策略详细信息	2924
策略版本	2924
JSON 策略文档	2925
了解更多信息	2926
IAMAccessAnalyzerReadOnlyAccess	2926
使用此策略	2926
策略详细信息	2926
策略版本	2926
JSON 策略文档	2926
了解更多信息	2927
IAMFullAccess	2927
使用此策略	2927
策略详细信息	2927
策略版本	2928
JSON 策略文档	2928
了解更多信息	2928

IAMReadOnlyAccess	2929
使用此策略	2929
策略详细信息	2929
策略版本	2929
JSON 策略文档	2929
了解更多信息	2930
IAMSelfManageServiceSpecificCredentials	2930
使用此策略	2930
策略详细信息	2930
策略版本	2930
JSON 策略文档	2931
了解更多信息	2931
IAMUserChangePassword	2931
使用此策略	2931
策略详细信息	2931
策略版本	2932
JSON 策略文档	2932
了解更多信息	2932
IAMUserSSHKeys	2933
使用此策略	2933
策略详细信息	2933
策略版本	2933
JSON 策略文档	2933
了解更多信息	2934
IVSFullAccess	2934
使用此策略	2934
策略详细信息	2934
策略版本	2934
JSON 策略文档	2935
了解更多信息	2935
IVSReadOnlyAccess	2935
使用此策略	2935
策略详细信息	2935
策略版本	2936
JSON 策略文档	2936
了解更多信息	2937

IVSRecordToS3	2937
使用此策略	2937
策略详细信息	2937
策略版本	2937
JSON 策略文档	2938
了解更多信息	2938
KafkaConnectServiceRolePolicy	2938
使用此策略	2938
策略详细信息	2938
策略版本	2939
JSON 策略文档	2939
了解更多信息	2940
KafkaServiceRolePolicy	2940
使用此策略	2941
策略详细信息	2941
策略版本	2941
JSON 策略文档	2941
了解更多信息	2942
KeyspacesReplicationServiceRolePolicy	2943
使用此策略	2943
策略详细信息	2943
策略版本	2943
JSON 策略文档	2943
了解更多信息	2944
LakeFormationDataAccessServiceRolePolicy	2944
使用此策略	2944
策略详细信息	2944
策略版本	2944
JSON 策略文档	2944
了解更多信息	2945
LexBotPolicy	2945
使用此策略	2945
策略详细信息	2945
策略版本	2945
JSON 策略文档	2946
了解更多信息	2946

LexChannelPolicy	2946
使用此策略	2947
策略详细信息	2947
策略版本	2947
JSON 策略文档	2947
了解更多信息	2947
LightsailExportAccess	2948
使用此策略	2948
策略详细信息	2948
策略版本	2948
JSON 策略文档	2948
了解更多信息	2949
MediaConnectGatewayInstanceRolePolicy	2949
使用此策略	2949
策略详细信息	2949
策略版本	2950
JSON 策略文档	2950
了解更多信息	2950
MediaPackageServiceRolePolicy	2950
使用此策略	2951
策略详细信息	2951
策略版本	2951
JSON 策略文档	2951
了解更多信息	2952
MemoryDBServiceRolePolicy	2952
使用此策略	2952
策略详细信息	2952
策略版本	2952
JSON 策略文档	2952
了解更多信息	2954
MigrationHubDMSAccessServiceRolePolicy	2954
使用此策略	2955
策略详细信息	2955
策略版本	2955
JSON 策略文档	2955
了解更多信息	2956

MigrationHubServiceRolePolicy	2956
使用此策略	2956
策略详细信息	2956
策略版本	2957
JSON 策略文档	2957
了解更多信息	2958
MigrationHubSMSAccessServiceRolePolicy	2958
使用此策略	2958
策略详细信息	2958
策略版本	2959
JSON 策略文档	2959
了解更多信息	2960
MonitronServiceRolePolicy	2960
使用此策略	2960
策略详细信息	2960
策略版本	2960
JSON 策略文档	2960
了解更多信息	2961
NeptuneConsoleFullAccess	2961
使用此策略	2961
策略详细信息	2961
策略版本	2962
JSON 策略文档	2962
了解更多信息	2967
NeptuneFullAccess	2967
使用此策略	2968
策略详细信息	2968
策略版本	2968
JSON 策略文档	2968
了解更多信息	2972
NeptuneGraphReadOnlyAccess	2972
使用此策略	2972
策略详细信息	2972
策略版本	2973
JSON 策略文档	2973
了解更多信息	2974

NeptuneReadOnlyAccess	2974
使用此策略	2975
策略详细信息	2975
策略版本	2975
JSON 策略文档	2975
了解更多信息	2977
NetworkAdministrator	2977
使用此策略	2978
策略详细信息	2978
策略版本	2978
JSON 策略文档	2978
了解更多信息	2985
OAMFullAccess	2985
使用此策略	2985
策略详细信息	2985
策略版本	2985
JSON 策略文档	2985
了解更多信息	2986
OAMReadOnlyAccess	2986
使用此策略	2986
策略详细信息	2986
策略版本	2986
JSON 策略文档	2987
了解更多信息	2987
OpensearchIngestionSelfManagedVpcePolicy	2987
使用此策略	2987
策略详细信息	2987
策略版本	2988
JSON 策略文档	2988
了解更多信息	2989
PartnerCentralAccountManagementUserRoleAssociation	2989
使用此策略	2989
策略详细信息	2989
策略版本	2989
JSON 策略文档	2989
了解更多信息	2990

PowerUserAccess	2990
使用此策略	2990
策略详细信息	2991
策略版本	2991
JSON 策略文档	2991
了解更多信息	2992
QBusinessServiceRolePolicy	2992
使用此策略	2992
策略详细信息	2992
策略版本	2992
JSON 策略文档	2992
了解更多信息	2994
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	2994
使用此策略	2994
策略详细信息	2994
策略版本	2995
JSON 策略文档	2995
了解更多信息	2995
RDSCloudHsmAuthorizationRole	2996
使用此策略	2996
策略详细信息	2996
策略版本	2996
JSON 策略文档	2996
了解更多信息	2997
ReadOnlyAccess	2997
使用此策略	2997
策略详细信息	2997
策略版本	2997
JSON 策略文档	2998
了解更多信息	3047
ResourceGroupsandTagEditorFullAccess	3047
使用此策略	3047
策略详细信息	3048
策略版本	3048
JSON 策略文档	3048
了解更多信息	3048

ResourceGroupsandTagEditorReadOnlyAccess	3049
使用此策略	3049
策略详细信息	3049
策略版本	3049
JSON 策略文档	3049
了解更多信息	3050
ResourceGroupsServiceRolePolicy	3050
使用此策略	3050
策略详细信息	3050
策略版本	3051
JSON 策略文档	3051
了解更多信息	3051
ROSAAmazonEBSCSIDriverOperatorPolicy	3051
使用此策略	3051
策略详细信息	3052
策略版本	3052
JSON 策略文档	3052
了解更多信息	3055
ROSACloudNetworkConfigOperatorPolicy	3055
使用此策略	3055
策略详细信息	3055
策略版本	3056
JSON 策略文档	3056
了解更多信息	3057
ROSAControlPlaneOperatorPolicy	3057
使用此策略	3057
策略详细信息	3057
策略版本	3057
JSON 策略文档	3058
了解更多信息	3062
ROSAImageRegistryOperatorPolicy	3062
使用此策略	3062
策略详细信息	3062
策略版本	3063
JSON 策略文档	3063
了解更多信息	3064

ROSAIngressOperatorPolicy	3064
使用此策略	3064
策略详细信息	3065
策略版本	3065
JSON 策略文档	3065
了解更多信息	3066
ROSAInstallerPolicy	3066
使用此策略	3066
策略详细信息	3066
策略版本	3066
JSON 策略文档	3067
了解更多信息	3074
ROSAKMSProviderPolicy	3075
使用此策略	3075
策略详细信息	3075
策略版本	3075
JSON 策略文档	3075
了解更多信息	3076
ROSAKubeControllerPolicy	3076
使用此策略	3076
策略详细信息	3076
策略版本	3077
JSON 策略文档	3077
了解更多信息	3081
ROSAManageSubscription	3081
使用此策略	3081
策略详细信息	3082
策略版本	3082
JSON 策略文档	3082
了解更多信息	3083
ROSANodePoolManagementPolicy	3083
使用此策略	3083
策略详细信息	3083
策略版本	3083
JSON 策略文档	3084
了解更多信息	3089

ROSASRESupportPolicy	3089
使用此策略	3090
策略详细信息	3090
策略版本	3090
JSON 策略文档	3090
了解更多信息	3095
ROSAWorkerInstancePolicy	3095
使用此策略	3095
策略详细信息	3095
策略版本	3095
JSON 策略文档	3096
了解更多信息	3096
Route53RecoveryReadinessServiceRolePolicy	3096
使用此策略	3096
策略详细信息	3096
策略版本	3097
JSON 策略文档	3097
了解更多信息	3100
Route53ResolverServiceRolePolicy	3100
使用此策略	3101
策略详细信息	3101
策略版本	3101
JSON 策略文档	3101
了解更多信息	3102
S3StorageLensServiceRolePolicy	3102
使用此策略	3102
策略详细信息	3102
策略版本	3102
JSON 策略文档	3102
了解更多信息	3103
SecretsManagerReadWrite	3103
使用此策略	3103
策略详细信息	3103
策略版本	3104
JSON 策略文档	3104
了解更多信息	3105

SecurityAudit	3106
使用此策略	3106
策略详细信息	3106
策略版本	3106
JSON 策略文档	3106
了解更多信息	3123
SecurityLakeServiceLinkedRole	3124
使用此策略	3124
策略详细信息	3124
策略版本	3124
JSON 策略文档	3124
了解更多信息	3127
ServerMigration_ServiceRole	3127
使用此策略	3127
策略详细信息	3127
策略版本	3128
JSON 策略文档	3128
了解更多信息	3133
ServerMigrationConnector	3133
使用此策略	3133
策略详细信息	3133
策略版本	3133
JSON 策略文档	3133
了解更多信息	3135
ServerMigrationServiceConsoleFullAccess	3135
使用此策略	3135
策略详细信息	3135
策略版本	3136
JSON 策略文档	3136
了解更多信息	3137
ServerMigrationServiceLaunchRole	3138
使用此策略	3138
策略详细信息	3138
策略版本	3138
JSON 策略文档	3138
了解更多信息	3141

ServerMigrationServiceRoleForInstanceValidation	3141
使用此策略	3141
策略详细信息	3141
策略版本	3142
JSON 策略文档	3142
了解更多信息	3142
ServiceQuotasFullAccess	3142
使用此策略	3143
策略详细信息	3143
策略版本	3143
JSON 策略文档	3143
了解更多信息	3145
ServiceQuotasReadOnlyAccess	3145
使用此策略	3145
策略详细信息	3145
策略版本	3145
JSON 策略文档	3146
了解更多信息	3147
ServiceQuotasServiceRolePolicy	3147
使用此策略	3147
策略详细信息	3147
策略版本	3147
JSON 策略文档	3147
了解更多信息	3148
SimpleWorkflowFullAccess	3148
使用此策略	3148
策略详细信息	3148
策略版本	3148
JSON 策略文档	3149
了解更多信息	3149
SplitCostAllocationDataServiceRolePolicy	3149
使用此策略	3149
策略详细信息	3149
策略版本	3150
JSON 策略文档	3150
了解更多信息	3150

SupportUser	3151
使用此策略	3151
策略详细信息	3151
策略版本	3151
JSON 策略文档	3151
了解更多信息	3156
SystemAdministrator	3156
使用此策略	3157
策略详细信息	3157
策略版本	3157
JSON 策略文档	3157
了解更多信息	3163
TranslateFullAccess	3163
使用此策略	3163
策略详细信息	3163
策略版本	3164
JSON 策略文档	3164
了解更多信息	3164
TranslateReadOnly	3165
使用此策略	3165
策略详细信息	3165
策略版本	3165
JSON 策略文档	3165
了解更多信息	3166
ViewOnlyAccess	3166
使用此策略	3166
策略详细信息	3166
策略版本	3166
JSON 策略文档	3167
了解更多信息	3175
VMImportExportRoleForAWSConnector	3175
使用此策略	3176
策略详细信息	3176
策略版本	3176
JSON 策略文档	3176
了解更多信息	3177

VPCLatticeFullAccess	3177
使用此策略	3177
策略详细信息	3177
策略版本	3177
JSON 策略文档	3178
了解更多信息	3180
VPCLatticeReadOnlyAccess	3180
使用此策略	3180
策略详细信息	3180
策略版本	3180
JSON 策略文档	3180
了解更多信息	3181
VPCLatticeServicesInvokeAccess	3181
使用此策略	3182
策略详细信息	3182
策略版本	3182
JSON 策略文档	3182
了解更多信息	3182
WAFLoggingServiceRolePolicy	3183
使用此策略	3183
策略详细信息	3183
策略版本	3183
JSON 策略文档	3183
了解更多信息	3184
WAFRegionalLoggingServiceRolePolicy	3184
使用此策略	3184
策略详细信息	3184
策略版本	3184
JSON 策略文档	3184
了解更多信息	3185
WAFV2LoggingServiceRolePolicy	3185
使用此策略	3185
策略详细信息	3185
策略版本	3186
JSON 策略文档	3186
了解更多信息	3186

WellArchitectedConsoleFullAccess	3186
使用此策略	3187
策略详细信息	3187
策略版本	3187
JSON 策略文档	3187
了解更多信息	3187
WellArchitectedConsoleReadOnlyAccess	3188
使用此策略	3188
策略详细信息	3188
策略版本	3188
JSON 策略文档	3188
了解更多信息	3189
WorkLinkServiceRolePolicy	3189
使用此策略	3189
策略详细信息	3189
策略版本	3189
JSON 策略文档	3190
了解更多信息	3190
.....	mmmcxci

什么是 AWS 托管策略？

AWS 托管策略是由 AWS 创建和管理的独立策略。AWS 托管策略旨在为许多常见使用案例提供权限。与必须自己编写策略相比，通过托管策略可以更轻松地将权限分配给用户、组和角色。

请记住，AWS 托管策略可能不会为您的特定使用场景授予最低权限许可，因为它们可供所有 AWS 客户使用。建议通过定义特定于您的应用场景的[客户托管策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新在 AWS 托管策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)。

了解策略参考页面

每个策略参考页面均包含以下信息：

- 使用此策略 – 是否可以将此策略附加到用户、组和角色
- 策略详细信息
 - 类型 - AWS 托管策略的类型
 - AWS managed policy – 标准 AWS 托管策略
 - Job function policy – 贴合行业中常用工作职能的策略
 - Service-linked role policy – 附加到服务相关角色的策略允许服务代表您执行操作，例如 [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
 - Service role policy – 旨在与服务角色配合使用的策略，例如 [the section called “AWSControlTowerServiceRolePolicy”](#)
 - 创建时间 – 首次创建此策略的时间
 - 编辑时间 – 编辑此版本策略的时间
 - ARN – 策略的 Amazon 资源名称
- 策略版本 – 策略授予的权限版本
- JSON 策略文档 – 策略 JSON
- 了解更多 – 与 AWS 托管策略相关的文档链接

已弃用的 AWS 托管策略

AWS 定期更新 AWS 托管策略。大多数情况下，我们会向策略添加权限。当推出新的服务或功能时，我们会添加权限。为了提高 AWS 托管策略的安全性，我们有时会减小策略的范围。在删除策略权限后，我们将该策略设置为已弃用状态，并提供一个新的可用策略。在 AWS 弃用某项服务或功能后，我们也会弃用该功能的 AWS 托管策略。

如果您收到一封电子邮件通知，告知您正在使用的策略已弃用，我们建议您立即采取行动。确定策略的变更并更新您的工作流。如果 AWS 提供了替代策略，则计划将其附加到所有受影响的身份（用户、组和角色），然后将已弃用的策略与这些身份分离。

已弃用的策略具有以下特性：

- 已从本指南中删除。
- 对于所有当前已附加该策略的身份，权限仍然有效。
- 在已附加该策略的身份所在的账户中，该策略将显示在 IAM 控制台的策略列表中，旁边有一个警告图标。
- 它无法附加至任何新身份。该策略若与当前身份分离则不能重新附加。
- 在与所有当前实体分离以后，该策略将不再显示。

AWS 托管策略

AWS 托管策略

- [AccessAnalyzerServiceRolePolicy](#)
- [AdministratorAccess](#)
- [AdministratorAccess-Amplify](#)
- [AdministratorAccess-AWSElasticBeanstalk](#)
- [AlexaForBusinessDeviceSetup](#)
- [AlexaForBusinessFullAccess](#)
- [AlexaForBusinessGatewayExecution](#)
- [AlexaForBusinessLifesizeDelegatedAccessPolicy](#)
- [AlexaForBusinessNetworkProfileServicePolicy](#)
- [AlexaForBusinessPolyDelegatedAccessPolicy](#)
- [AlexaForBusinessReadOnlyAccess](#)
- [AmazonAPIGatewayAdministrator](#)
- [AmazonAPIGatewayInvokeFullAccess](#)
- [AmazonAPIGatewayPushToCloudWatchLogs](#)
- [AmazonAppFlowFullAccess](#)
- [AmazonAppFlowReadOnlyAccess](#)
- [AmazonAppStreamFullAccess](#)
- [AmazonAppStreamPCAAccess](#)
- [AmazonAppStreamReadOnlyAccess](#)
- [AmazonAppStreamServiceAccess](#)
- [AmazonAthenaFullAccess](#)
- [AmazonAugmentedAIFullAccess](#)
- [AmazonAugmentedAIHumanLoopFullAccess](#)
- [AmazonAugmentedAIIntegratedAPIAccess](#)
- [AmazonBedrockFullAccess](#)
- [AmazonBedrockReadOnly](#)

- [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](#)
- [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](#)
- [AmazonDynamoDBFullAccesswithDataPipeline](#)
- [AmazonDynamoDBReadOnlyAccess](#)
- [AmazonEBSCSIDriverPolicy](#)
- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AmazonEC2ContainerServiceAutoscaleRole](#)
- [AmazonEC2ContainerServiceEventsRole](#)

- [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](#)
- [AmazonFISServiceRolePolicy](#)
- [AmazonForecastFullAccess](#)
- [AmazonFraudDetectorFullAccessPolicy](#)
- [AmazonFreeRTOSFullAccess](#)
- [AmazonFreeRTOSOTAUpdate](#)
- [AmazonFSxConsoleFullAccess](#)
- [AmazonFSxConsoleReadOnlyAccess](#)
- [AmazonFSxFullAccess](#)
- [AmazonFSxReadOnlyAccess](#)
- [AmazonFSxServiceRolePolicy](#)
- [AmazonGlacierFullAccess](#)
- [AmazonGlacierReadOnlyAccess](#)
- [AmazonGrafanaAthenaAccess](#)
- [AmazonGrafanaCloudWatchAccess](#)
- [AmazonGrafanaRedshiftAccess](#)

- [AmazonGrafanaServiceLinkedRolePolicy](#)
- [AmazonGuardDutyFullAccess](#)
- [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#)
- [AmazonGuardDutyReadOnlyAccess](#)
- [AmazonGuardDutyServiceRolePolicy](#)
- [AmazonHealthLakeFullAccess](#)
- [AmazonHealthLakeReadOnlyAccess](#)
- [AmazonHoneycodeFullAccess](#)
- [AmazonHoneycodeReadOnlyAccess](#)
- [AmazonHoneycodeServiceRolePolicy](#)
- [AmazonHoneycodeTeamAssociationFullAccess](#)
- [AmazonHoneycodeTeamAssociationReadOnlyAccess](#)
- [AmazonHoneycodeWorkbookFullAccess](#)
- [AmazonHoneycodeWorkbookReadOnlyAccess](#)
- [AmazonInspector2AgentlessServiceRolePolicy](#)
- [AmazonInspector2FullAccess](#)
- [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](#)
- [AmazonOmicsFullAccess](#)
- [AmazonOmicsReadOnlyAccess](#)
- [AmazonOneEnterpriseFullAccess](#)
- [AmazonOneEnterpriseInstallerAccess](#)
- [AmazonOneEnterpriseReadOnlyAccess](#)
- [AmazonOpenSearchDashboardsServiceRolePolicy](#)
- [AmazonOpenSearchDirectQueryGlueCreateAccess](#)
- [AmazonOpenSearchIngestionFullAccess](#)
- [AmazonOpenSearchIngestionReadOnlyAccess](#)
- [AmazonOpenSearchIngestionServiceRolePolicy](#)
- [AmazonOpenSearchServerlessServiceRolePolicy](#)
- [AmazonOpenSearchServiceCognitoAccess](#)
- [AmazonOpenSearchServiceFullAccess](#)
- [AmazonOpenSearchServiceReadOnlyAccess](#)
- [AmazonOpenSearchServiceRolePolicy](#)
- [AmazonPersonalizeFullAccess](#)
- [AmazonPollyFullAccess](#)
- [AmazonPollyReadOnlyAccess](#)
- [AmazonPrometheusConsoleFullAccess](#)
- [AmazonPrometheusFullAccess](#)
- [AmazonPrometheusQueryAccess](#)
- [AmazonPrometheusRemoteWriteAccess](#)
- [AmazonPrometheusScraperServiceRolePolicy](#)
- [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](#)
- [AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy](#)
- [AmazonSageMakerCanvasAIServicesAccess](#)
- [AmazonSageMakerCanvasBedrockAccess](#)
- [AmazonSageMakerCanvasDataPrepFullAccess](#)
- [AmazonSageMakerCanvasDirectDeployAccess](#)
- [AmazonSageMakerCanvasForecastAccess](#)
- [AmazonSageMakerCanvasFullAccess](#)
- [AmazonSageMakerClusterInstanceRolePolicy](#)

- [AmazonSageMakerCoreServiceRolePolicy](#)
- [AmazonSageMakerEdgeDeviceFleetPolicy](#)
- [AmazonSageMakerFeatureStoreAccess](#)
- [AmazonSageMakerFullAccess](#)
- [AmazonSageMakerGeospatialExecutionRole](#)
- [AmazonSageMakerGeospatialFullAccess](#)
- [AmazonSageMakerGroundTruthExecution](#)
- [AmazonSageMakerMechanicalTurkAccess](#)
- [AmazonSageMakerModelGovernanceUseAccess](#)
- [AmazonSageMakerModelRegistryFullAccess](#)
- [AmazonSageMakerNotebooksServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy](#)
- [AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy](#)
- [AmazonSageMakerPipelinesIntegrations](#)
- [AmazonSageMakerReadOnly](#)
- [AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy](#)
- [AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy](#)
- [AmazonSecurityLakeAdministrator](#)
- [AmazonSecurityLakeMetastoreManager](#)
- [AmazonSecurityLakePermissionsBoundary](#)
- [AmazonSESEFullAccess](#)
- [AmazonSESReadOnlyAccess](#)

- [AmazonSESServiceRolePolicy](#)
- [AmazonSNSFullAccess](#)
- [AmazonSNSReadOnlyAccess](#)
- [AmazonSNSRole](#)
- [AmazonSQSFullAccess](#)
- [AmazonSQSReadOnlyAccess](#)
- [AmazonSSMAutomationApproverAccess](#)
- [AmazonSSMAutomationRole](#)
- [AmazonSSMDirectoryServiceAccess](#)
- [AmazonSSMFullAccess](#)
- [AmazonSSMMaintenanceWindowRole](#)
- [AmazonSSMManagedEC2InstanceDefaultPolicy](#)
- [AmazonSSMManagedInstanceCore](#)
- [AmazonSSMPatchAssociation](#)
- [AmazonSSMReadOnlyAccess](#)
- [AmazonSSMServiceRolePolicy](#)
- [AmazonSumerianFullAccess](#)
- [AmazonTextractFullAccess](#)
- [AmazonTextractServiceRole](#)
- [AmazonTimestreamConsoleFullAccess](#)
- [AmazonTimestreamFullAccess](#)
- [AmazonTimestreamInfluxDBFullAccess](#)
- [AmazonTimestreamInfluxDBServiceRolePolicy](#)
- [AmazonTimestreamReadOnlyAccess](#)
- [AmazonTranscribeFullAccess](#)
- [AmazonTranscribeReadOnlyAccess](#)
- [AmazonVPCCrossAccountNetworkInterfaceOperations](#)
- [AmazonVPCFullAccess](#)
- [AmazonVPCNetworkAccessAnalyzerFullAccessPolicy](#)

- [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)
- [AmazonVPCReachabilityAnalyzerPathComponentReadPolicy](#)
- [AmazonVPCReadOnlyAccess](#)
- [AmazonWorkDocsFullAccess](#)
- [AmazonWorkDocsReadOnlyAccess](#)
- [AmazonWorkMailEventsServiceRolePolicy](#)
- [AmazonWorkMailFullAccess](#)
- [AmazonWorkMailMessageFlowFullAccess](#)
- [AmazonWorkMailMessageFlowReadOnlyAccess](#)
- [AmazonWorkMailReadOnlyAccess](#)
- [AmazonWorkSpacesAdmin](#)
- [AmazonWorkSpacesApplicationManagerAdminAccess](#)
- [AmazonWorkspacesPCAAccess](#)
- [AmazonWorkSpacesSelfServiceAccess](#)
- [AmazonWorkSpacesServiceAccess](#)
- [AmazonWorkSpacesWebReadOnly](#)
- [AmazonWorkSpacesWebServiceRolePolicy](#)
- [AmazonZocaloFullAccess](#)
- [AmazonZocaloReadOnlyAccess](#)
- [AmplifyBackendDeployFullAccess](#)
- [APIGatewayServiceRolePolicy](#)
- [AppIntegrationsServiceLinkedRolePolicy](#)
- [ApplicationAutoScalingForAmazonAppStreamAccess](#)
- [ApplicationDiscoveryServiceContinuousExportServiceRolePolicy](#)
- [AppRunnerNetworkingServiceRolePolicy](#)
- [AppRunnerServiceRolePolicy](#)
- [AutoScalingConsoleFullAccess](#)
- [AutoScalingConsoleReadOnlyAccess](#)
- [AutoScalingFullAccess](#)

- [AutoScalingNotificationAccessRole](#)
- [AutoScalingReadOnlyAccess](#)
- [AutoScalingServiceRolePolicy](#)
- [AWS_ConfigRole](#)
- [AWSAccountActivityAccess](#)
- [AWSAccountManagementFullAccess](#)
- [AWSAccountManagementReadOnlyAccess](#)
- [AWSAccountUsageReportAccess](#)
- [AWSAgentlessDiscoveryService](#)
- [AWSAppFabricFullAccess](#)
- [AWSAppFabricReadOnlyAccess](#)
- [AWSAppFabricServiceRolePolicy](#)
- [AWSApplicationAutoscalingAppStreamFleetPolicy](#)
- [AWSApplicationAutoscalingCassandraTablePolicy](#)
- [AWSApplicationAutoscalingComprehendEndpointPolicy](#)
- [AWSApplicationAutoScalingCustomResourcePolicy](#)
- [AWSApplicationAutoscalingDynamoDBTablePolicy](#)
- [AWSApplicationAutoscalingEC2SpotFleetRequestPolicy](#)
- [AWSApplicationAutoscalingECSServicePolicy](#)
- [AWSApplicationAutoscalingElastiCacheRGPPolicy](#)
- [AWSApplicationAutoscalingEMRInstanceGroupPolicy](#)
- [AWSApplicationAutoscalingKafkaClusterPolicy](#)
- [AWSApplicationAutoscalingLambdaConcurrencyPolicy](#)
- [AWSApplicationAutoscalingNeptuneClusterPolicy](#)
- [AWSApplicationAutoscalingRDSClusterPolicy](#)
- [AWSApplicationAutoscalingSageMakerEndpointPolicy](#)
- [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](#)
- [AWSArtifactReportsReadOnlyAccess](#)

- [AWSArtifactServiceRolePolicy](#)
- [AWSAuditManagerAdministratorAccess](#)
- [AWSAuditManagerServiceRolePolicy](#)
- [AWSAutoScalingPlansEC2AutoScalingPolicy](#)
- [AWSBackupAuditAccess](#)
- [AWSBackupDataTransferAccess](#)
- [AWSBackupFullAccess](#)
- [AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync](#)
- [AWSBackupOperatorAccess](#)
- [AWSBackupOrganizationAdminAccess](#)
- [AWSBackupRestoreAccessForSAPHANA](#)
- [AWSBackupServiceLinkedRolePolicyForBackup](#)
- [AWSBackupServiceLinkedRolePolicyForBackupTest](#)
- [AWSBackupServiceRolePolicyForBackup](#)
- [AWSBackupServiceRolePolicyForRestores](#)
- [AWSBackupServiceRolePolicyForS3Backup](#)
- [AWSBackupServiceRolePolicyForS3Restore](#)
- [AWSBatchFullAccess](#)
- [AWSBatchServiceEventTargetRole](#)
- [AWSBatchServiceRole](#)
- [AWSBCMDDataExportsServiceRolePolicy](#)
- [AWSBillingConductorFullAccess](#)
- [AWSBillingConductorReadOnlyAccess](#)
- [AWSBillingReadOnlyAccess](#)
- [AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM](#)
- [AWSBudgetsActionsWithAWSResourceControlAccess](#)
- [AWSBudgetsReadOnlyAccess](#)
- [AWSBugBustFullAccess](#)
- [AWSBugBustPlayerAccess](#)

- [AWSBugBustServiceRolePolicy](#)
- [AWSCertificateManagerFullAccess](#)
- [AWSCertificateManagerPrivateCAAuditor](#)
- [AWSCertificateManagerPrivateCAFullAccess](#)
- [AWSCertificateManagerPrivateCAPrivilegedUser](#)
- [AWSCertificateManagerPrivateCARedOnly](#)
- [AWSCertificateManagerPrivateCAUser](#)
- [AWSCertificateManagerReadOnly](#)
- [AWSChatbotServiceLinkedRolePolicy](#)
- [AWSCleanRoomsFullAccess](#)
- [AWSCleanRoomsFullAccessNoQuerying](#)
- [AWSCleanRoomsMLFullAccess](#)
- [AWSCleanRoomsMLReadOnlyAccess](#)
- [AWSCleanRoomsReadOnlyAccess](#)
- [AWSCloud9Administrator](#)
- [AWSCloud9EnvironmentMember](#)
- [AWSCloud9ServiceRolePolicy](#)
- [AWSCloud9SSMInstanceProfile](#)
- [AWSCloud9User](#)
- [AWSCloudFormationFullAccess](#)
- [AWSCloudFormationReadOnlyAccess](#)
- [AWSCloudFrontLogger](#)
- [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](#)
- [AWSConfigMultiAccountSetupPolicy](#)
- [AWSConfigRemediationServiceRolePolicy](#)
- [AWSConfigRoleForOrganizations](#)
- [AWSConfigRulesExecutionRole](#)
- [AWSConfigServiceRolePolicy](#)
- [AWSConfigUserAccess](#)
- [AWSConnector](#)
- [AWSControlTowerAccountServiceRolePolicy](#)
- [AWSControlTowerServiceRolePolicy](#)
- [AWSCostAndUsageReportAutomationPolicy](#)
- [AWSDataExchangeFullAccess](#)
- [AWSDataExchangeProviderFullAccess](#)
- [AWSDataExchangeReadOnly](#)
- [AWSDataExchangeSubscriberFullAccess](#)
- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWSDataPipeline_FullAccess](#)
- [AWSDataPipeline_PowerUser](#)
- [AWSDataSyncDiscoveryServiceRolePolicy](#)
- [AWSDataSyncFullAccess](#)
- [AWSDataSyncReadOnlyAccess](#)
- [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](#)
- [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](#)
- [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](#)
- [AWSIoTClickFullAccess](#)
- [AWSIoTClickReadOnlyAccess](#)
- [AWSIoTAnalyticsFullAccess](#)
- [AWSIoTAnalyticsReadOnlyAccess](#)
- [AWSIoTConfigAccess](#)
- [AWSIoTConfigReadOnlyAccess](#)
- [AWSIoTDataAccess](#)
- [AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction](#)
- [AWSIoTDeviceDefenderAudit](#)
- [AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction](#)
- [AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction](#)
- [AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateCACertMitigationAction](#)
- [AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction](#)
- [AWSIoTDeviceTesterForFreeRTOSFullAccess](#)
- [AWSIoTDeviceTesterForGreengrassFullAccess](#)
- [AWSIOTEventsFullAccess](#)
- [AWSIOTEventsReadOnlyAccess](#)
- [AWSIOTFleetHubFederationAccess](#)
- [AWSIOTFleetwiseServiceRolePolicy](#)
- [AWSIOTFullAccess](#)
- [AWSIOTLogging](#)
- [AWSIOTOTAUpdate](#)
- [AWSIoTRoboRunnerFullAccess](#)

- [AWSIoTRoboRunnerReadOnly](#)
- [AWSIoTRoboRunnerServiceRolePolicy](#)
- [AWSIoTRuleActions](#)
- [AWSIoTSiteWiseConsoleFullAccess](#)
- [AWSIoTSiteWiseFullAccess](#)
- [AWSIoTSiteWiseMonitorPortalAccess](#)
- [AWSIoTSiteWiseMonitorServiceRolePolicy](#)
- [AWSIoTSiteWiseReadOnlyAccess](#)
- [AWSIoTThingsRegistration](#)
- [AWSIoTThingMakerServiceRolePolicy](#)
- [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](#)
- [AWSManagedServicesDeploymentToolkitPolicy](#)
- [AWSMarketplaceAmiIngestion](#)
- [AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWSMarketplaceFullAccess](#)
- [AWSMarketplaceGetEntitlements](#)
- [AWSMarketplaceImageBuildFullAccess](#)
- [AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWSMarketplaceManageSubscriptions](#)
- [AWSMarketplaceMeteringFullAccess](#)
- [AWSMarketplaceMeteringRegisterUsage](#)
- [AWSMarketplaceProcurementSystemAdminFullAccess](#)

- [AWSMarketplacePurchaseOrdersServiceRolePolicy](#)
- [AWSMarketplaceRead-only](#)
- [AWSMarketplaceResaleAuthorizationServiceRolePolicy](#)
- [AWSMarketplaceSellerFullAccess](#)
- [AWSMarketplaceSellerProductsFullAccess](#)
- [AWSMarketplaceSellerProductsReadOnly](#)
- [AWSMediaConnectServicePolicy](#)
- [AWSMediaTailorServiceRolePolicy](#)
- [AWSMigrationHubDiscoveryAccess](#)
- [AWSMigrationHubDMSAccess](#)
- [AWSMigrationHubFullAccess](#)
- [AWSMigrationHubOrchestratorConsoleFullAccess](#)
- [AWSMigrationHubOrchestratorInstanceRolePolicy](#)
- [AWSMigrationHubOrchestratorPlugin](#)
- [AWSMigrationHubOrchestratorServiceRolePolicy](#)
- [AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess](#)
- [AWSMigrationHubRefactorSpaces-SSMAutomationPolicy](#)
- [AWSMigrationHubRefactorSpacesFullAccess](#)
- [AWSMigrationHubRefactorSpacesServiceRolePolicy](#)
- [AWSMigrationHubSMSAccess](#)
- [AWSMigrationHubStrategyCollector](#)
- [AWSMigrationHubStrategyConsoleFullAccess](#)
- [AWSMigrationHubStrategyServiceRolePolicy](#)
- [AWSMobileHub_FullAccess](#)
- [AWSMobileHub_ReadOnly](#)
- [AWSMSKReplicatorExecutionRole](#)
- [AWSNetworkFirewallServiceRolePolicy](#)
- [AWSNetworkManagerCloudWANServiceRolePolicy](#)
- [AWSNetworkManagerFullAccess](#)
- [AWSNetworkManagerReadOnlyAccess](#)

- [AWSNetworkManagerServiceRolePolicy](#)
- [AWSOpsWorks_FullAccess](#)
- [AWSOpsWorksCloudWatchLogs](#)
- [AWSOpsWorksCMInstanceProfileRole](#)
- [AWSOpsWorksCMServiceRole](#)
- [AWSOpsWorksInstanceRegistration](#)
- [AWSOpsWorksRegisterCLI_EC2](#)
- [AWSOpsWorksRegisterCLI_OnPremises](#)
- [AWSOrganizationsFullAccess](#)
- [AWSOrganizationsReadOnlyAccess](#)
- [AWSOrganizationsServiceTrustPolicy](#)
- [AWSOutpostsAuthorizeServerPolicy](#)
- [AWSOutpostsServiceRolePolicy](#)
- [AWSPanoramaApplianceRolePolicy](#)
- [AWSPanoramaApplianceServiceRolePolicy](#)
- [AWSPanoramaFullAccess](#)
- [AWSPanoramaGreengrassGroupRolePolicy](#)
- [AWSPanoramaSageMakerRolePolicy](#)
- [AWSPanoramaServiceLinkedRolePolicy](#)
- [AWSPanoramaServiceRolePolicy](#)
- [AWSPriceListServiceFullAccess](#)
- [AWSPrivateCAAuditor](#)
- [AWSPrivateCAFullAccess](#)
- [AWSPrivateCAPrivilegedUser](#)
- [AWSPrivateCARedOnly](#)
- [AWSPrivateCAUser](#)
- [AWSPrivateMarketplaceAdminFullAccess](#)
- [AWSPrivateMarketplaceRequests](#)
- [AWSPrivateNetworksServiceRolePolicy](#)
- [AWSProtonCodeBuildProvisioningBasicAccess](#)

- [AWSProtonCodeBuildProvisioningServiceRolePolicy](#)
- [AWSProtonDeveloperAccess](#)
- [AWSProtonFullAccess](#)
- [AWSProtonReadOnlyAccess](#)
- [AWSProtonServiceGitSyncServiceRolePolicy](#)
- [AWSProtonSyncServiceRolePolicy](#)
- [AWSPurchaseOrdersServiceRolePolicy](#)
- [AWSQuickSightAssetBundleExportPolicy](#)
- [AWSQuickSightAssetBundleImportPolicy](#)
- [AWSQuicksightAthenaAccess](#)
- [AWSQuickSightDescribeRDS](#)
- [AWSQuickSightDescribeRedshift](#)
- [AWSQuickSightElasticsearchPolicy](#)
- [AWSQuickSightIoTAnalyticsAccess](#)
- [AWSQuickSightListIAM](#)
- [AWSQuicksightOpenSearchPolicy](#)
- [AWSQuickSightSageMakerPolicy](#)
- [AWSQuickSightTimestreamPolicy](#)
- [AWSReachabilityAnalyzerServiceRolePolicy](#)
- [AWSRefactoringToolkitFullAccess](#)
- [AWSRefactoringToolkitSidecarPolicy](#)
- [AWSrePostPrivateCloudWatchAccess](#)
- [AWSRepostSpaceSupportOperationsPolicy](#)
- [AWSResilienceHubAssessmentExecutionPolicy](#)
- [AWSResourceAccessManagerFullAccess](#)
- [AWSResourceAccessManagerReadOnlyAccess](#)
- [AWSResourceAccessManagerResourceShareParticipantAccess](#)
- [AWSResourceAccessManagerServiceRolePolicy](#)
- [AWSResourceExplorerFullAccess](#)
- [AWSResourceExplorerOrganizationsAccess](#)

- [AWSResourceExplorerReadOnlyAccess](#)
- [AWSResourceExplorerServiceRolePolicy](#)
- [AWSResourceGroupsReadOnlyAccess](#)
- [AWSRoboMaker_FullAccess](#)
- [AWSRoboMakerReadOnlyAccess](#)
- [AWSRoboMakerServicePolicy](#)
- [AWSRoboMakerServiceRolePolicy](#)
- [AWSRolesAnywhereServicePolicy](#)
- [AWSS3OnOutpostsServiceRolePolicy](#)
- [AWSSavingsPlansFullAccess](#)
- [AWSSavingsPlansReadOnlyAccess](#)
- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)
- [AWSSecurityHubReadOnlyAccess](#)
- [AWSSecurityHubServiceRolePolicy](#)
- [AWSServiceCatalogAdminFullAccess](#)
- [AWSServiceCatalogAdminReadOnlyAccess](#)
- [AWSServiceCatalogAppRegistryFullAccess](#)
- [AWSServiceCatalogAppRegistryReadOnlyAccess](#)
- [AWSServiceCatalogAppRegistryServiceRolePolicy](#)
- [AWSServiceCatalogEndUserFullAccess](#)
- [AWSServiceCatalogEndUserReadOnlyAccess](#)
- [AWSServiceCatalogOrgsDataSyncServiceRolePolicy](#)
- [AWSServiceCatalogSyncServiceRolePolicy](#)
- [AWSServiceRoleForAmazonEKSNodegroup](#)
- [AWSServiceRoleForAmazonQDeveloper](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy](#)
- [AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy](#)
- [AWSServiceRoleForCodeGuru-Profiler](#)
- [AWSServiceRoleForCodeWhispererPolicy](#)

- [AWSServiceRoleForEC2ScheduledInstances](#)
- [AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy](#)
- [AWSServiceRoleForImageBuilder](#)
- [AWSServiceRoleForIoTSiteWise](#)
- [AWSServiceRoleForLogDeliveryPolicy](#)
- [AWSServiceRoleForMonitronPolicy](#)
- [AWSServiceRoleForNeptuneGraphPolicy](#)
- [AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWSServiceRoleForSMS](#)
- [AWSServiceRoleForUserSubscriptions](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)
- [AWSShieldDRTAccessPolicy](#)
- [AWSShieldServiceRolePolicy](#)
- [AWSSSMForSAPServiceLinkedRolePolicy](#)
- [AWSSSMOpsInsightsServiceRolePolicy](#)
- [AWSSSODirectoryAdministrator](#)
- [AWSSSODirectoryReadOnly](#)
- [AWSSSOMasterAccountAdministrator](#)
- [AWSSSOMemberAccountAdministrator](#)
- [AWSSSOReadOnly](#)
- [AWSSSOServiceRolePolicy](#)
- [AWSStepFunctionsConsoleFullAccess](#)
- [AWSStepFunctionsFullAccess](#)
- [AWSStepFunctionsReadOnlyAccess](#)
- [AWSStorageGatewayFullAccess](#)
- [AWSStorageGatewayReadOnlyAccess](#)
- [AWSStorageGatewayServiceRolePolicy](#)
- [AWSSupplyChainFederationAdminAccess](#)
- [AWSsupportAccess](#)

- [AWSSupportAppFullAccess](#)
- [AWSSupportAppReadOnlyAccess](#)
- [AWSSupportPlansFullAccess](#)
- [AWSSupportPlansReadOnlyAccess](#)
- [AWSSupportServiceRolePolicy](#)
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSSystemsManagerChangeManagementServicePolicy](#)
- [AWSSystemsManagerForSAPFullAccess](#)
- [AWSSystemsManagerForSAPReadOnlyAccess](#)
- [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](#)
- [BatchServiceRolePolicy](#)
- [Billing](#)
- [CertificateManagerServiceRolePolicy](#)
- [ClientVPNServiceConnectionsRolePolicy](#)
- [ClientVPNServiceRolePolicy](#)
- [CloudFormationStackSetsOrgAdminServiceRolePolicy](#)
- [CloudFormationStackSetsOrgMemberServiceRolePolicy](#)
- [CloudFrontFullAccess](#)
- [CloudFrontReadOnlyAccess](#)
- [CloudHSMServiceRolePolicy](#)
- [CloudSearchFullAccess](#)
- [CloudSearchReadOnlyAccess](#)

- [CloudTrailServiceRolePolicy](#)
- [CloudWatch-CrossAccountAccess](#)
- [CloudWatchActionsEC2Access](#)
- [CloudWatchAgentAdminPolicy](#)
- [CloudWatchAgentServerPolicy](#)
- [CloudWatchApplicationInsightsFullAccess](#)
- [CloudWatchApplicationInsightsReadOnlyAccess](#)
- [CloudwatchApplicationInsightsServiceLinkedRolePolicy](#)
- [CloudWatchApplicationSignalsFullAccess](#)
- [CloudWatchApplicationSignalsReadOnlyAccess](#)
- [CloudWatchApplicationSignalsServiceRolePolicy](#)
- [CloudWatchAutomaticDashboardsAccess](#)
- [CloudWatchCrossAccountSharingConfiguration](#)
- [CloudWatchEventsBuiltInTargetExecutionAccess](#)
- [CloudWatchEventsFullAccess](#)
- [CloudWatchEventsInvocationAccess](#)
- [CloudWatchEventsReadOnlyAccess](#)
- [CloudWatchEventsServiceRolePolicy](#)
- [CloudWatchFullAccess](#)
- [CloudWatchFullAccessV2](#)
- [CloudWatchInternetMonitorServiceRolePolicy](#)
- [CloudWatchLambdaInsightsExecutionRolePolicy](#)
- [CloudWatchLogsCrossAccountSharingConfiguration](#)
- [CloudWatchLogsFullAccess](#)
- [CloudWatchLogsReadOnlyAccess](#)
- [CloudWatchNetworkMonitorServiceRolePolicy](#)
- [CloudWatchReadOnlyAccess](#)
- [CloudWatchSyntheticsFullAccess](#)
- [CloudWatchSyntheticsReadOnlyAccess](#)
- [ComprehendDataAccessRolePolicy](#)

- [ComprehendFullAccess](#)
- [ComprehendMedicalFullAccess](#)
- [ComprehendReadOnly](#)
- [ComputeOptimizerReadOnlyAccess](#)
- [ComputeOptimizerServiceRolePolicy](#)
- [ConfigConformsServiceRolePolicy](#)
- [CostOptimizationHubAdminAccess](#)
- [CostOptimizationHubReadOnlyAccess](#)
- [CostOptimizationHubServiceRolePolicy](#)
- [CustomerProfilesServiceLinkedRolePolicy](#)
- [DatabaseAdministrator](#)
- [DataScientist](#)
- [DAXServiceRolePolicy](#)
- [DynamoDBCloudWatchContributorInsightsServiceRolePolicy](#)
- [DynamoDBKinesisReplicationServiceRolePolicy](#)
- [DynamoDBReplicationServiceRolePolicy](#)
- [EC2FastLaunchFullAccess](#)
- [EC2FastLaunchServiceRolePolicy](#)
- [EC2FleetTimeShiftableServiceRolePolicy](#)
- [EC2ImageBuilderCrossAccountDistributionAccess](#)
- [EC2ImageBuilderLifecycleExecutionPolicy](#)
- [EC2InstanceConnect](#)
- [EC2InstanceConnectEndpoint](#)
- [EC2InstanceProfileForImageBuilder](#)
- [EC2InstanceProfileForImageBuilderECRContainerBuilds](#)
- [ECRReplicationServiceRolePolicy](#)
- [ElastiCacheServiceRolePolicy](#)
- [ElasticLoadBalancingFullAccess](#)
- [ElasticLoadBalancingReadOnly](#)
- [ElementalActivationsDownloadSoftwareAccess](#)

- [ElementalActivationsFullAccess](#)
- [ElementalActivationsGenerateLicenses](#)
- [ElementalActivationsReadOnlyAccess](#)
- [ElementalAppliancesSoftwareFullAccess](#)
- [ElementalAppliancesSoftwareReadOnlyAccess](#)
- [ElementalSupportCenterFullAccess](#)
- [EMRDescribeClusterPolicyForEMRWAL](#)
- [FMSServiceRolePolicy](#)
- [FSxDeleteServiceLinkedRoleAccess](#)
- [GameLiftGameServerGroupPolicy](#)
- [GlobalAcceleratorFullAccess](#)
- [GlobalAcceleratorReadOnlyAccess](#)
- [GreengrassOTAUpdateArtifactAccess](#)
- [GroundTruthSyntheticConsoleFullAccess](#)
- [GroundTruthSyntheticConsoleReadOnlyAccess](#)
- [Health_OrganizationsServiceRolePolicy](#)
- [IAMAccessAdvisorReadOnly](#)
- [IAMAccessAnalyzerFullAccess](#)
- [IAMAccessAnalyzerReadOnlyAccess](#)
- [IAMFullAccess](#)
- [IAMReadOnlyAccess](#)
- [IAMSelfManageServiceSpecificCredentials](#)
- [IAMUserChangePassword](#)
- [IAMUserSSHKeys](#)
- [IVSFullAccess](#)
- [IVSReadOnlyAccess](#)
- [IVSRecordToS3](#)
- [KafkaConnectServiceRolePolicy](#)
- [KafkaServiceRolePolicy](#)
- [KeyspacesReplicationServiceRolePolicy](#)

- [LakeFormationDataAccessServiceRolePolicy](#)
- [LexBotPolicy](#)
- [LexChannelPolicy](#)
- [LightsailExportAccess](#)
- [MediaConnectGatewayInstanceRolePolicy](#)
- [MediaPackageServiceRolePolicy](#)
- [MemoryDBServiceRolePolicy](#)
- [MigrationHubDMSAccessServiceRolePolicy](#)
- [MigrationHubServiceRolePolicy](#)
- [MigrationHubSMSAccessServiceRolePolicy](#)
- [MonitronServiceRolePolicy](#)
- [NeptuneConsoleFullAccess](#)
- [NeptuneFullAccess](#)
- [NeptuneGraphReadOnlyAccess](#)
- [NeptuneReadOnlyAccess](#)
- [NetworkAdministrator](#)
- [OAMFullAccess](#)
- [OAMReadOnlyAccess](#)
- [OpensearchIngestionSelfManagedVpcePolicy](#)
- [PartnerCentralAccountManagementUserRoleAssociation](#)
- [PowerUserAccess](#)
- [QBusinessServiceRolePolicy](#)
- [QuickSightAccessForS3StorageManagementAnalyticsReadOnly](#)
- [RDSCloudHsmAuthorizationRole](#)
- [ReadOnlyAccess](#)
- [ResourceGroupsandTagEditorFullAccess](#)
- [ResourceGroupsandTagEditorReadOnlyAccess](#)
- [ResourceGroupsServiceRolePolicy](#)
- [ROSAAmazonEBSCSIDriverOperatorPolicy](#)
- [ROSACloudNetworkConfigOperatorPolicy](#)

- [ROSAControlPlaneOperatorPolicy](#)
- [ROSAImageRegistryOperatorPolicy](#)
- [ROSAIngressOperatorPolicy](#)
- [ROSAInstallerPolicy](#)
- [ROSAKMSProviderPolicy](#)
- [ROSAKubeControllerPolicy](#)
- [ROSAManageSubscription](#)
- [ROSANodePoolManagementPolicy](#)
- [ROSASRESupportPolicy](#)
- [ROSAWorkerInstancePolicy](#)
- [Route53RecoveryReadinessServiceRolePolicy](#)
- [Route53ResolverServiceRolePolicy](#)
- [S3StorageLensServiceRolePolicy](#)
- [SecretsManagerReadWrite](#)
- [SecurityAudit](#)
- [SecurityLakeServiceLinkedRole](#)
- [ServerMigration_ServiceRole](#)
- [ServerMigrationConnector](#)
- [ServerMigrationServiceConsoleFullAccess](#)
- [ServerMigrationServiceLaunchRole](#)
- [ServerMigrationServiceRoleForInstanceValidation](#)
- [ServiceQuotasFullAccess](#)
- [ServiceQuotasReadOnlyAccess](#)
- [ServiceQuotasServiceRolePolicy](#)
- [SimpleWorkflowFullAccess](#)
- [SplitCostAllocationDataServiceRolePolicy](#)
- [SupportUser](#)
- [SystemAdministrator](#)
- [TranslateFullAccess](#)
- [TranslateReadOnly](#)

- [ViewOnlyAccess](#)
- [VMImportExportRoleForAWSConnector](#)
- [VPCLatticeFullAccess](#)
- [VPCLatticeReadOnlyAccess](#)
- [VPCLatticeServicesInvokeAccess](#)
- [WAFLoggingServiceRolePolicy](#)
- [WAFRegionalLoggingServiceRolePolicy](#)
- [WAFV2LoggingServiceRolePolicy](#)
- [WellArchitectedConsoleFullAccess](#)
- [WellArchitectedConsoleReadOnlyAccess](#)
- [WorkLinkServiceRolePolicy](#)

AccessAnalyzerServiceRolePolicy

描述：允许访问分析器分析资源元数据

AccessAnalyzerServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 2 日 17:13 UTC
- 编辑时间：世界标准时间 2024 年 5 月 30 日 18:34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "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:GetBucketPolicy",
    "s3express:ListAllMyDirectoryBuckets",
    "sns:GetTopicAttributes",
    "sns:ListTopics",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:ListSecrets",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AdministratorAccess

描述：提供对 AWS 服务和资源的完全访问权限。

AdministratorAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AdministratorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AdministratorAccess-Amplify

描述：授予账户管理权限，同时明确允许直接访问 Amplify 应用程序所需的资源。

AdministratorAccess-Amplify 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AdministratorAccess-Amplify 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2020 年 12 月 1 日 19:03 UTC
- 编辑时间：世界标准时间 2024 年 4 月 4 日 20:35
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-Amplify

策略版本

策略版本：v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AdministratorAccess-AWSElasticBeanstalk

描述：授予账户管理权限。明确允许开发人员和管理员直接访问管理 Elastic Beanstalk 应用程序所需的资源

AdministratorAccess-AWSElasticBeanstalk是一个[AWS 托管策略](#)。

使用此策略

您可以将 AdministratorAccess-AWSElasticBeanstalk 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 19:36 UTC
- 编辑时间：2023 年 3 月 23 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
      "StringLike" : {
        "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessDeviceSetup

描述：提供设备设置对 AlexaForBusiness 服务的访问权限

AlexaForBusinessDeviceSetup是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AlexaForBusinessDeviceSetup` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2019 年 5 月 20 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessFullAccess

描述：授予对资源的完全访问权限和对相关 AlexaForBusiness 资源的访问权限 AWS 服务

AlexaForBusinessFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AlexaForBusinessFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2020 年 7 月 1 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessGatewayExecution

描述：提供对 AlexaForBusiness 服务的网关执行访问权限

AlexaForBusinessGatewayExecution 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AlexaForBusinessGatewayExecution 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2017 年 11 月 30 日 16:47 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

描述：提供对 Lifesize AVS 设备的访问权限

AlexaForBusinessLifesizeDelegatedAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AlexaForBusinessLifesizeDelegatedAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 4 日 19:46 UTC
- 编辑时间：2020 年 6 月 12 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/
AlexaForBusinessLifesizeDelegatedAccessPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:DisassociateDeviceFromRoom",
      "a4b>DeleteDevice",
      "a4b:UpdateDevice",
      "a4b:GetDevice"
    ],
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:RegisterAVSDevice"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "a4b:amazonId" : [
          "A2IW07UEGWV4TL"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:SearchDevices"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "a4b:filters_deviceType" : [
          "*A2IW07UEGWV4TL"
        ]
      }
    }
  },

```

```
    "Null" : {
      "a4b:filters_deviceType" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:AssociateDeviceWithRoom"
    ],
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL",
      "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/*"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessNetworkProfileServicePolicy

描述：此策略允许 Alexa for Business 执行根据您的网络配置文件安排的自动任务。

AlexaForBusinessNetworkProfileServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 3 月 13 日 00:53 UTC
- 编辑时间：2019 年 4 月 5 日 21:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessPolyDelegatedAccessPolicy

描述：提供对 Poly AVS 设备的访问权限

AlexaForBusinessPolyDelegatedAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AlexaForBusinessPolyDelegatedAccessPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 16 日 19:48 UTC
- 编辑时间：2019 年 10 月 16 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b>DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWW36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
    }
  ]
}
```

```
"Effect" : "Allow",
"Resource" : [
  "*"
],
"Condition" : {
  "StringEquals" : {
    "a4b:amazonId" : [
      "A238TWW36W3S92",
      "A1FUZ1SC53VJXD"
    ]
  }
},
{
  "Action" : [
    "a4b:SearchDevices"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : [
    "a4b:AssociateDeviceWithRoom"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:a4b:us-east-1:*:device/*/*:A238TWW36W3S92",
    "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AlexaForBusinessReadOnlyAccess

描述：提供 AlexaForBusiness 服务的只读访问权限

AlexaForBusinessReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AlexaForBusinessReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2019 年 11 月 20 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAPIGatewayAdministrator

描述：提供通过在 Amazon API Gateway 中创建/编辑/删除 API 的完全访问权限。AWS Management Console

AmazonAPIGatewayAdministrator是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonAPIGatewayAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:34 UTC
- 编辑时间：2015 年 7 月 9 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAPIGatewayInvokeFullAccess

描述：提供在 Amazon API Gateway 中调用 API 的完全访问权限。

AmazonAPIGatewayInvokeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAPIGatewayInvokeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:36 UTC
- 编辑时间：2018 年 12 月 18 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAPIGatewayPushToCloudWatchLogs

描述：允许 API Gateway 将日志推送到用户的账户。

AmazonAPIGatewayPushToCloudWatchLogs 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAPIGatewayPushToCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 11 日 23:41 UTC
- 编辑时间：2015 年 11 月 11 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:DescribeLogGroups",
  "logs:DescribeLogStreams",
  "logs:PutLogEvents",
  "logs:GetLogEvents",
  "logs:FilterLogEvents"
],
"Resource" : "*"
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppFlowFullAccess

描述：提供对 Amazon 的完全访问权限 AppFlow 以及对作为流量源或目标支持的 AWS 服务 (S3 和 Redshift) 的访问权限。还提供对 KMS 的访问权限以进行加密

AmazonAppFlowFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppFlowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 2 日 23:30 UTC
- 编辑时间：2022 年 2 月 28 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppFlowReadOnlyAccess

描述：提供对亚马逊 Appflow 流程的只读访问权限

AmazonAppFlowReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppFlowReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 2 日 23:26 UTC
- 编辑时间：2022 年 2 月 28 日 20:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppStreamFullAccess

描述：提供 AppStream 通过 Amazon 的完全访问权限 AWS Management Console。

AmazonAppStreamFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppStreamFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 8 月 28 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppStreamPCAAccess

描述：Amazon AppStream 2.0 访问客户账户中的 Certificate Manager 私有 CA 进行基于证书的身份验证 AWS

AmazonAppStreamPCAAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppStreamPCAAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建日期：2022 年 10 月 24 日 17:05 UTC
- 编辑时间：2022 年 10 月 24 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppStreamReadOnlyAccess

描述：AppStream 通过提供对 Amazon 的只读访问权限 AWS Management Console。

AmazonAppStreamReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppStreamReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2016 年 12 月 7 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAppStreamServiceAccess

描述：Amazon AppStream 服务角色的默认策略。

AmazonAppStreamServiceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAppStreamServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间 : 2016 年 11 月 19 日 04:17 UTC
- 编辑时间 : 2020 年 6 月 26 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAthenaFullAccess

描述：提供对 Amazon Athena 的完全访问权限以及对启用查询、写入结果和数据管理所需的依赖项的限定访问权限。

AmazonAthenaFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAthenaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 16:46 UTC

- 编辑时间：世界标准时间 2024 年 1 月 3 日 19:05
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "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",
    "glue:StartColumnStatisticsTaskRun",
    "glue:GetColumnStatisticsTaskRun",
    "glue:GetColumnStatisticsTaskRuns"
  ],
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAugmentedAIFullAccess

描述：提供执行所有操作的权限 Amazon Augmented AI 资源 FlowDefinitions，包括、HumanTaskUis 和 HumanLoops。不允许访问 FlowDefinitions 针对公众人群 Workteam 进行创作。

AmazonAugmentedAIFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonAugmentedAIFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:21 UTC
- 编辑时间：2019 年 12 月 3 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAugmentedAIHumanLoopFullAccess

描述：提供对执行所有操作的访问权限 HumanLoops。

AmazonAugmentedAIHumanLoopFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAugmentedAIHumanLoopFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2019 年 12 月 3 日 16:20 UTC
- 编辑时间：2019 年 12 月 3 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonAugmentedAIIntegratedAPIAccess

描述：提供执行所有操作的权限 Amazon Agumented AI 资源 FlowDefinitions，包括、HumanTaskUis 和 HumanLoops。还提供对与 Amazon Agumented AI 集成的服务的相关操作的访问权限。

AmazonAugmentedAIIntegratedAPIAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonAugmentedAIIntegratedAPIAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 22 日 20:47 UTC
- 编辑时间：2020 年 4 月 22 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonBedrockFullAccess

描述：提供对 Amazon Bedrock 的完全访问权限以及对其所需的相关服务的有限访问权限

AmazonBedrockFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonBedrockFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 15:47
- 编辑时间：世界标准时间 2023 年 12 月 6 日 15:47
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonBedrockReadOnly

描述：提供对 Amazon Bedrock 的只读访问权限

AmazonBedrockReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonBedrockReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 15:48
- 编辑时间：世界标准时间 2023 年 12 月 6 日 15:48
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",

```

```
        "bedrock:ListCustomModels",
        "bedrock:GetCustomModel",
        "bedrock:ListTagsForResource",
        "bedrock:GetFoundationModelAvailability"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonBraketFullAccess

描述：提供通过 AWS Management Console 和软件开发工具包对 Amazon Braket 的完全访问权限。还提供对相关服务（例如 S3、日志）的访问权限。

AmazonBraketFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonBraketFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 6 日 20:12 UTC
- 编辑时间：2023 年 4 月 19 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketFullAccess

策略版本

策略版本：v6（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData"
      ],
      "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"
    }
  }
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonBraketJobsExecutionPolicy

描述：授予访问权限 AWS 服务 和执行 Amazon Braket Job 所需的资源，包括 S3、Cloudwatch、IAM 和 Braket

AmazonBraketJobsExecutionPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonBraketJobsExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 26 日 19:34 UTC
- 编辑时间：2021 年 11 月 28 日 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
    }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonBraketServiceRolePolicy

描述：允许 Amazon Braket 代表您创建和管理 AWS 资源

AmazonBraketServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 4 日 17:12 UTC
- 编辑时间：2020 年 8 月 6 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeFullAccess

描述：通过提供对 Amazon Chime 管理控制台的完全访问权限。AWS Management Console

AmazonChimeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonChimeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 1 日 22:15 UTC
- 编辑时间：2020 年 12 月 14 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeReadOnly

描述：通过提供对 Amazon Chime 管理控制台的只读访问权限。AWS Management Console

AmazonChimeReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonChimeReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 1 日 22:04 UTC
- 编辑时间：2020 年 12 月 14 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeReadOnly

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeSDK

描述：提供对 Amazon Chime 软件开发工具包操作的访问权限

AmazonChimeSDK是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonChimeSDK 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 2 月 4 日 21:53 UTC
- 编辑时间：2023 年 1 月 10 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

描述：亚马逊 Chime SDK MediaPipelines 服务关联角色的托管策略

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 4 月 4 日 22:02 UTC
- 编辑时间：世界标准时间 2023 年 12 月 8 日 19:14
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeSDKMessagingServiceRolePolicy

描述：允许 Amazon Chime SDK Messaging 访问 AWS 资源并启用消息传递功能

AmazonChimeSDKMessagingServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 3 日 01:43 UTC
- 编辑时间：2023 年 3 月 3 日 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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-*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeServiceRolePolicy

描述：允许访问由 Amazon Chime 使用或管理的 AWS 资源

AmazonChimeServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 9 月 30 日 22:25 UTC
- 编辑时间：2019 年 9 月 30 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

描述：允许 Amazon Chime 代表你访问亚马逊 Transcribe 和 Amazon Transcribe Medical

AmazonChimeTranscriptionServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 4 日 21:47 UTC
- 编辑时间：2021 年 8 月 4 日 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeUserManagement

描述：通过提供对 Amazon Chime 管理控制台的用户管理权限。AWS Management Console

AmazonChimeUserManagement 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonChimeUserManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 1 日 22:17 UTC
- 编辑时间：2020 年 2 月 18 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
        "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

描述：适用于 Amazon Chime 的服务关联角色的托管策略 VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 9 月 30 日 22:16 UTC
- 编辑时间：2023 年 4 月 14 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudDirectoryFullAccess

描述：提供对亚马逊 Cloud Directory 服务的完全访问权限。

AmazonCloudDirectoryFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudDirectoryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 25 日 00:41 UTC
- 编辑时间：2017 年 2 月 25 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudDirectoryReadOnlyAccess

描述：提供对亚马逊 Cloud Directory 服务的只读访问权限。

AmazonCloudDirectoryReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudDirectoryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 28 日 23:42 UTC
- 编辑时间：2017 年 2 月 28 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "clouddirectory:List*",
      "clouddirectory:Get*",
      "clouddirectory:LookupPolicy",
      "clouddirectory:BatchRead"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchEvidentlyFullAccess

描述：CloudWatch 显然仅提供对 Amazon 的完全访问权限。还提供对相关亚马逊 S3、亚马逊 SNS CloudWatch、亚马逊和其他相关服务的访问权限。

AmazonCloudWatchEvidentlyFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudWatchEvidentlyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 15:10 UTC
- 编辑时间：2021 年 11 月 29 日 15:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

描述：CloudWatch 显然提供对 Amazon 的只读访问权限

AmazonCloudWatchEvidentlyReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudWatchEvidentlyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 15:08 UTC
- 编辑时间：2021 年 11 月 29 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

描述：允许 CloudWatch Evidently Service 代表客户管理相关 AWS 资源

AmazonCloudWatchEvidentlyServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 13 日 17:25 UTC
- 编辑时间：2022 年 9 月 13 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchRUMFullAccess

描述：授予 Amazon CloudWatch RUM 服务的完全访问权限

AmazonCloudWatchRUMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudWatchRUMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 15:46 UTC
- 编辑时间：2021 年 11 月 29 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchRUMReadOnlyAccess

描述：授予 Amazon CloudWatch RUM 服务的只读权限

AmazonCloudWatchRUMReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCloudWatchRUMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 11 月 29 日 15:43 UTC
- 编辑时间：2022 年 10 月 28 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCloudWatchRUMServiceRolePolicy

描述：授予 Amazon CloudWatch RUM 服务向其他相关 AWS 服务发布监控数据的权限

AmazonCloudWatchRUMServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型**：服务相关角色策略
- **创建时间**：2021 年 11 月 17 日 23:17 UTC
- **编辑时间**：2023 年 2 月 22 日 20:35 UTC
- **ARN**: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeCatalystFullAccess

描述：提供对 Amazon 的完全访问权限 CodeCatalyst

AmazonCodeCatalystFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeCatalystFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 20 日 16:50 UTC
- 编辑时间：2023 年 4 月 20 日 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeCatalystReadOnlyAccess

描述：提供对 Amazon 的只读访问权限 CodeCatalyst

AmazonCodeCatalystReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeCatalystReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 20 日 16:49 UTC
- 编辑时间：2023 年 4 月 20 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "codecatalyst:Get*",
      "codecatalyst:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeCatalystSupportAccess

描述：允许 Amazon CodeCatalyst 代表您创建、更新和解决问题 AWS Support。

AmazonCodeCatalystSupportAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeCatalystSupportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 12:34 UTC
- 编辑时间：2023 年 4 月 20 日 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruProfilerAgentAccess

描述：提供 Amazon CodeGuru Profiler 代理所需的访问权限。

AmazonCodeGuruProfilerAgentAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruProfilerAgentAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 5 日 22:11 UTC
- 编辑时间：2022 年 5 月 5 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruProfilerFullAccess

描述：提供对 Amazon CodeGuru Profiler 的完全访问权限。

AmazonCodeGuruProfilerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruProfilerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 10:13 UTC
- 编辑时间：2020 年 7 月 15 日 03:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruProfilerReadOnlyAccess

描述：提供对 Amazon P CodeGuru profiler 的只读访问权限。

AmazonCodeGuruProfilerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruProfilerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 10:30 UTC
- 编辑时间：2020 年 6 月 27 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruReviewerFullAccess

描述：授予对 Amazon CodeGuru Reviewer 的完全访问权限和对所需依赖项的限定访问权限。

AmazonCodeGuruReviewerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruReviewerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 08:33 UTC
- 编辑时间：2020 年 8 月 29 日 04:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruReviewerReadOnlyAccess

描述：提供对 Amazon CodeGuru Reviewer 的只读访问权限。

AmazonCodeGuruReviewerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruReviewerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 08:48 UTC
- 编辑时间：2020 年 8 月 29 日 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruReviewerServiceRolePolicy

描述：Amazon CodeGuru Reviewer 代表您访问资源所需的服务相关角色。

AmazonCodeGuruReviewerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 05:31 UTC
- 编辑时间：2020 年 11 月 27 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruSecurityFullAccess

描述：提供对 Amazon CodeGuru 安全的完全访问权限。

AmazonCodeGuruSecurityFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruSecurityFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 9 日 21:03 UTC
- 编辑时间：2023 年 5 月 9 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCodeGuruSecurityScanAccess

描述：提供处理 Amazon CodeGuru 安全扫描所需的访问权限。

AmazonCodeGuruSecurityScanAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCodeGuruSecurityScanAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 9 日 20:54 UTC
- 编辑时间：2023 年 5 月 9 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoDeveloperAuthenticatedIdentities

描述：提供对 Amazon Cognito API 的访问权限，以支持通过身份验证后端进行开发者身份验证的身份。

AmazonCognitoDeveloperAuthenticatedIdentities 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCognitoDeveloperAuthenticatedIdentities 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 3 月 24 日 17:22 UTC
- 编辑时间：2015 年 3 月 24 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoIdpEmailServiceRolePolicy

描述：允许 Amazon Cognito 用户池服务使用你的 SES 身份发送电子邮件

AmazonCognitoIdpEmailServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 3 月 21 日 21:32 UTC
- 编辑时间：2019 年 3 月 21 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoIdpServiceRolePolicy

描述：允许访问 Amazon Cognito 用户池 AWS 服务 及其使用或管理的资源

AmazonCognitoIdpServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2020 年 6 月 26 日 22:30 UTC
- 编辑时间：2020 年 6 月 26 日 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoPowerUser

描述：提供对现有 Amazon Cognito 资源的管理权限。您需要 AWS 账户 管理员权限才能创建新的 Cognito 资源。

AmazonCognitoPowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCognitoPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 3 月 24 日 17:14 UTC
- 编辑时间：2021 年 6 月 1 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "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*"
  ]
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoReadOnly

描述：提供对 Amazon Cognito 资源的只读访问权限。

AmazonCognitoReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonCognitoReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 3 月 24 日 17:06 UTC
- 编辑时间：2019 年 8 月 1 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

描述：此策略定义了 Cognito 身份池中未经身份验证的身份所允许的权限集。本策略不用作独立的权限策略。它用作一种防护机制，防止对身份池中的角色附加过度宽松的策略。请勿将此策略附加至任何角色，因为 Cognito Identity Service 在创建凭证时会自动将其包含为限定范围的策略。现在，通过增强型流程临时访问其他 AWS 资源的权限将由与服务提供的未经身份验证的用户的身身份关联的角色与 Cognito 拥有的此托管策略中赋予的权限的交集来定义。

AmazonCognitoUnAuthedIdentitiesSessionPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCognitoUnAuthedIdentitiesSessionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 19 日 23:04 UTC

- 编辑时间：2023 年 7 月 19 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonCognitoUnauthenticatedIdentities

描述：此策略定义了 Cognito 身份池中未经身份验证的身份所允许的权限集。无需将其附加到您的未经身份验证的角色，因为 Cognito Identity Service 在创建凭证时会自动将其包含为限定范围的策略。现在，通过增强型流程临时访问其他 AWS 资源的权限将由与服务提供的未经身份验证的用户的身份关联的角色与 Cognito 拥有的此托管策略中赋予的权限的交集来定义。

AmazonCognitoUnauthenticatedIdentities 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonCognitoUnauthenticatedIdentities 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 1 日 22:36 UTC
- 编辑时间：2023 年 2 月 1 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnect_FullAccess

描述：此策略的目的是向 AWS Connect 用户授予使用 Connect 资源所需的权限。此策略提供通过 C AWS onnect 控制台和公共 API 对 Connect 资源的完全访问权限

AmazonConnect_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonConnect_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 19:54 UTC
- 编辑时间：2023 年 3 月 7 日 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

描述：Amazon Connect 活动服务关联角色的政策

AmazonConnectCampaignsServiceLinkedRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 23 日 20:54 UTC
- 编辑时间：2023 年 11 月 8 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnectReadOnlyAccess

描述：授予查看您中的 Amazon Connect 实例的权限 AWS 账户。

AmazonConnectReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonConnectReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 17 日 21:00 UTC
- 编辑时间：2019 年 11 月 6 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

```
    "connect:Describe*",
    "connect:List*",
    "ds:DescribeDirectories"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Deny",
  "Action" : "connect:GetFederationTokens",
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnectServiceLinkedRolePolicy

描述：允许 Amazon Connect 代表您创建和管理 AWS 资源。

AmazonConnectServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 9 月 7 日 00:21 UTC
- 编辑时间：世界标准时间 2024 年 5 月 24 日 01:42
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy

策略版本

策略版本：v16 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
},
{
  "Sid" : "AllowReadPermissionForCustomerProfileObjects",
  "Effect" : "Allow",
  "Action" : [
    "profile:ListProfileObjects",
    "profile:GetProfileObjectType"
  ],
  "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"
  ],
  "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" : "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/*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnectSynchronizationServiceRolePolicy

描述：允许 Amazon Connect 代表您跨区域同步 AWS 资源。

AmazonConnectSynchronizationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 10 月 27 日 22:38 UTC
- 编辑时间：2023 年 10 月 27 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect:DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect:DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",
        "connect:CreateAgentStatus",
        "connect:UpdateAgentStatus",
        "connect:DescribeAgentStatus",
        "connect:ListAgentStatuses",
        "connect:CreateQuickConnect",
        "connect:UpdateQuickConnect*",
        "connect:DeleteQuickConnect",
        "connect:DescribeQuickConnect",
        "connect:ListQuickConnects",
        "connect:CreateHoursOfOperation",
        "connect:UpdateHoursOfOperation",
        "connect:DeleteHoursOfOperation",
        "connect:DescribeHoursOfOperation",
        "connect:ListHoursOfOperations",
        "connect:CreateQueue",
        "connect:UpdateQueue*",
        "connect:DeleteQueue",

```

```

    "connect:DescribeQueue",
    "connect:ListQueue*",
    "connect:CreatePrompt",
    "connect:UpdatePrompt",
    "connect>DeletePrompt",
    "connect:DescribePrompt",
    "connect:ListPrompts",
    "connect:GetPromptFile",
    "connect:CreateSecurityProfile",
    "connect:UpdateSecurityProfile",
    "connect>DeleteSecurityProfile",
    "connect:DescribeSecurityProfile",
    "connect:ListSecurityProfile*",
    "connect:CreateContactFlow*",
    "connect:UpdateContactFlow*",
    "connect>DeleteContactFlow*",
    "connect:DescribeContactFlow*",
    "connect:ListContactFlow*",
    "connect:BatchGetFlowAssociation",
    "connect:CreatePredefinedAttribute",
    "connect:UpdatePredefinedAttribute",
    "connect>DeletePredefinedAttribute",
    "connect:DescribePredefinedAttribute",
    "connect:ListPredefinedAttributes",
    "connect:ListTagsForResource",
    "connect:TagResource",
    "connect:UntagResource",
    "connect:ListTrafficDistributionGroups",
    "connect:ListPhoneNumbersV2",
    "connect:UpdatePhoneNumber",
    "connect:DescribePhoneNumber",
    "connect:Associate*",
    "connect:Disassociate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPutMetricsForConnectNamespace",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Connect"
    }
  }
}

```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonConnectVoiceIDFullAccess

描述：提供对 Amazon Connect 语音识别的完全访问权限

AmazonConnectVoiceIDFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonConnectVoiceIDFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 26 日 19:04 UTC
- 编辑时间：2021 年 9 月 26 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneDomainExecutionRolePolicy

描述：Amazon DomainExecutionRole 服务角色 DataZone 的默认策略。亚马逊使用此角色 DataZone 对亚马逊 DataZone 域中的数据进行分类、发现、管理、共享和分析。

AmazonDataZoneDomainExecutionRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneDomainExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 27 日 21:55 UTC
- 编辑时间：世界标准时间 2024 年 4 月 1 日 19:25
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone>DeleteTimeSeriesDataPoints",
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone>CreateAsset",
        "datazone>CreateAssetRevision",
        "datazone>CreateAssetType",
        "datazone:CreateDataSource",
        "datazone>CreateEnvironment",
        "datazone>CreateEnvironmentBlueprint",
        "datazone>CreateEnvironmentProfile",
        "datazone>CreateFormType",
        "datazone>CreateGlossary",
        "datazone>CreateGlossaryTerm",
        "datazone>CreateListingChangeSet",
        "datazone>CreateProject",
        "datazone>CreateProjectMembership",
        "datazone>CreateSubscriptionGrant",
        "datazone>CreateSubscriptionRequest",
        "datazone>DeleteAsset",
        "datazone>DeleteAssetType",
        "datazone>DeleteDataSource",
        "datazone>DeleteEnvironment",
        "datazone>DeleteEnvironmentBlueprint",
        "datazone>DeleteEnvironmentProfile",
```

```
"datazone:DeleteFormType",
"datazone:DeleteGlossary",
"datazone:DeleteGlossaryTerm",
"datazone:DeleteListing",
"datazone:DeleteProject",
"datazone:DeleteProjectMembership",
"datazone:DeleteSubscriptionGrant",
"datazone:DeleteSubscriptionRequest",
"datazone:DeleteSubscriptionTarget",
"datazone:GetAsset",
"datazone:GetAssetType",
"datazone:GetDataSource",
"datazone:GetDataSourceRun",
"datazone:GetDomain",
"datazone:GetEnvironment",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentBlueprint",
"datazone:GetEnvironmentCredentials",
"datazone:GetEnvironmentProfile",
"datazone:GetFormType",
"datazone:GetGlossary",
"datazone:GetGlossaryTerm",
"datazone:GetGroupProfile",
"datazone:GetListing",
"datazone:GetProject",
"datazone:GetSubscription",
"datazone:GetSubscriptionEligibility",
"datazone:GetSubscriptionGrant",
"datazone:GetSubscriptionRequestDetails",
"datazone:GetSubscriptionTarget",
"datazone:GetUserProfile",
"datazone:ListAccountEnvironments",
"datazone:ListAssetRevisions",
"datazone:ListDataSourceRunActivities",
"datazone:ListDataSourceRuns",
"datazone:ListDataSources",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:ListEnvironmentBlueprintConfigurationSummaries",
"datazone:ListEnvironmentBlueprints",
"datazone:ListEnvironmentProfiles",
"datazone:ListEnvironments",
"datazone:ListGroupsForUser",
"datazone:ListNotifications",
"datazone:ListProjectMemberships",
```

```
"datazone:ListProjects",
"datazone:ListSubscriptionGrants",
"datazone:ListSubscriptionRequests",
"datazone:ListSubscriptionTargets",
"datazone:ListSubscriptions",
"datazone:ListWarehouseMetadata",
"datazone:RejectPredictions",
"datazone:RejectSubscriptionRequest",
"datazone:RevokeSubscription",
"datazone:Search",
"datazone:SearchGroupProfiles",
"datazone:SearchListings",
"datazone:SearchTypes",
"datazone:SearchUserProfiles",
"datazone:StartDataSourceRun",
"datazone:UpdateDataSource",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentBlueprint",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:UpdateEnvironmentProfile",
"datazone:UpdateGlossary",
"datazone:UpdateGlossaryTerm",
"datazone:UpdateProject",
"datazone:UpdateSubscriptionGrantStatus",
"datazone:UpdateSubscriptionRequest",
"datazone:StartMetadataGenerationRun",
"datazone:GetMetadataGenerationRun",
"datazone:CancelMetadataGenerationRun",
"datazone:ListMetadataGenerationRuns"
],
"Resource" : "*"
},
{
  "Sid" : "RAMResourceShareStatement",
  "Effect" : "Allow",
  "Action" : "ram:GetResourceShareAssociations",
  "Resource" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

描述：Amazon 为环境 DataZone 创建 IAM 角色以执行数据分析操作，并在创建这些角色时使用此策略来定义其权限边界。

AmazonDataZoneEnvironmentRolePermissionsBoundary 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneEnvironmentRolePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 11 日 23:38 UTC
- 编辑时间：世界标准时间 2023 年 11 月 17 日 23:29
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : [
    "datzone:*",
    "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" : [
  "*"
]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneFullAccess

描述：DataZone 通过提供对 Amazon 的完全访问权限 AWS Management Console 以及对亚马逊所需的相关服务的有限访问权限。

AmazonDataZoneFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 22 日 20:06 UTC
- 编辑时间：世界标准时间 2024 年 4 月 23 日 21:36
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "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*"
},
{
  "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"
    ],
    "Resource" : "*"
},
{
    "Sid" : "IAMPassRoleStatement",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:passedToService" : "datazone.amazonaws.com"
        }
    }
}

```

```
    }
  },
  {
    "Sid" : "IAMGetPolicyStatement",
    "Effect" : "Allow",
    "Action" : "iam:GetPolicy",
    "Resource" : [
      "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
    ]
  },
  {
    "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_*"
      },
      "Null" : {
        "aws:TagKeys" : "false"
      }
    }
  },
  {
    "Sid" : "CreateSecretStatement",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager::*:secret:AmazonDataZone-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
      }
    }
  }
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneFullUserAccess

描述：提供对 Amazon 的完全访问权限 DataZone，但不允许管理域名、用户或关联账户。

AmazonDataZoneFullUserAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneFullUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 22 日 21:06 UTC
- 编辑时间：世界标准时间 2024 年 4 月 1 日 19:27
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AmazonDataZoneUserOperations",
    "Effect" : "Allow",
    "Action" : [
      "datazone:PostTimeSeriesDataPoints",
      "datazone:ListTimeSeriesDataPoints",
      "datazone:GetTimeSeriesDataPoint",
      "datazone>DeleteTimeSeriesDataPoints",
      "datazone:GetDomain",
      "datazone:CreateFormType",
      "datazone:GetFormType",
      "datazone:GetIamPortalLoginUrl",
      "datazone:SearchUserProfiles",
      "datazone:SearchGroupProfiles",
      "datazone:GetUserProfile",
      "datazone:GetGroupProfile",
      "datazone:ListGroupsForUser",
      "datazone>DeleteFormType",
      "datazone:CreateAssetType",
      "datazone:GetAssetType",
      "datazone>DeleteAssetType",
      "datazone:CreateGlossary",
      "datazone:GetGlossary",
      "datazone>DeleteGlossary",
      "datazone:UpdateGlossary",
      "datazone:CreateGlossaryTerm",
      "datazone:GetGlossaryTerm",
      "datazone>DeleteGlossaryTerm",
      "datazone:UpdateGlossaryTerm",
      "datazone:CreateAsset",
      "datazone:GetAsset",
      "datazone>DeleteAsset",
      "datazone:CreateAssetRevision",
      "datazone:ListAssetRevisions",
      "datazone:AcceptPredictions",
      "datazone:RejectPredictions",
      "datazone:Search",
      "datazone:SearchTypes",
      "datazone:CreateListingChangeSet",
      "datazone>DeleteListing",
      "datazone:SearchListings",
      "datazone:GetListing",
```



```
"datazone:CreateDataSource",
"datazone:GetDataSource",
"datazone>DeleteDataSource",
"datazone:UpdateDataSource",
"datazone:ListDataSources",
"datazone:StartDataSourceRun",
"datazone:GetDataSourceRun",
"datazone:ListDataSourceRuns",
"datazone:ListDataSourceRunActivities",
"datazone:ListEnvironmentBlueprintConfigurations",
"datazone:CreateEnvironmentBlueprint",
"datazone:GetEnvironmentBlueprint",
"datazone>DeleteEnvironmentBlueprint",
"datazone:UpdateEnvironmentBlueprint",
"datazone:ListEnvironmentBlueprints",
"datazone:CreateProject",
"datazone:UpdateProject",
"datazone:GetProject",
"datazone>DeleteProject",
"datazone:ListProjects",
"datazone:CreateProjectMembership",
"datazone>DeleteProjectMembership",
"datazone:ListProjectMemberships",
"datazone:CreateEnvironmentProfile",
"datazone:GetEnvironmentProfile",
"datazone:UpdateEnvironmentProfile",
"datazone>DeleteEnvironmentProfile",
"datazone:ListEnvironmentProfiles",
"datazone:CreateEnvironment",
"datazone:GetEnvironment",
"datazone>DeleteEnvironment",
"datazone:UpdateEnvironment",
"datazone:UpdateEnvironmentDeploymentStatus",
"datazone:ListEnvironments",
"datazone:ListAccountEnvironments",
"datazone:GetEnvironmentActionLink",
"datazone:GetEnvironmentCredentials",
"datazone:GetSubscriptionTarget",
"datazone>DeleteSubscriptionTarget",
"datazone:ListSubscriptionTargets",
"datazone:CreateSubscriptionRequest",
"datazone:AcceptSubscriptionRequest",
"datazone:UpdateSubscriptionRequest",
"datazone:ListWarehouseMetadata",
```

```

    "datazone:RejectSubscriptionRequest",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:ListSubscriptionRequests",
    "datazone>DeleteSubscriptionRequest",
    "datazone:GetSubscription",
    "datazone:CancelSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:ListSubscriptions",
    "datazone:RevokeSubscription",
    "datazone>CreateSubscriptionGrant",
    "datazone>DeleteSubscriptionGrant",
    "datazone:GetSubscriptionGrant",
    "datazone:ListSubscriptionGrants",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:ListNotifications",
    "datazone:StartMetadataGenerationRun",
    "datazone:GetMetadataGenerationRun",
    "datazone:CancelMetadataGenerationRun",
    "datazone:ListMetadataGenerationRuns"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RAMResourceShareOperations",
  "Effect" : "Allow",
  "Action" : "ram:GetResourceShareAssociations",
  "Resource" : "*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneGlueManageAccessRolePolicy

描述：该政策授予允许 Amazon DataZone 启用发布和数据访问权限的权限。

AmazonDataZoneGlueManageAccessRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneGlueManageAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 22 日 20:21 UTC
- 编辑时间：世界标准时间 2024 年 6 月 3 日 23:29
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GlueTagDatabasePermissions",
      "Effect": "Allow",
      "Action": [
        "glue:TagResource",
        "glue:UntagResource",
        "glue:GetTags"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists": {
```

```
        "aws:TagKeys" : "DataZoneDiscoverable_*"
    }
}
},
{
    "Sid" : "GlueDataQualityPermissions",
    "Effect" : "Allow",
    "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
    ],
    "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "GlueTableDatabasePermissions",
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "LakeformationResourceSharingPermissions",
    "Effect" : "Allow",
    "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
```

```

    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation>DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CrossAccountRAMResourceSharingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "ram.amazonaws.com"
      ]
    }
  }
},
{
  "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" : "CrossAccountRAMResourceShareInvitationPermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram>DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram>ListResourceSharePermissions",
    "ram:UpdateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:ResourceShareName" : [
        "LakeFormation*"
      ]
    }
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "lakeformation.amazonaws.com"
    ]
  }
}
```

```
    }
  }
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
  "Effect" : "Allow",
  "Action" : "ram:AssociateResourceSharePermission",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "lakeformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSDecryptPermission",
  "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*"
  ]
},
{
```

```
"Sid" : "PassRoleForDataLocationRegistration",
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "arn:aws:iam::*:role/AmazonDataZone*",
  "arn:aws:iam::*:role/service-role/AmazonDataZone*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "lakeformation.amazonaws.com"
    ]
  }
}
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZonePortalFullAccessPolicy

描述：提供对亚马逊 DataZone API 的完全访问权限

AmazonDataZonePortalFullAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZonePortalFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 3 月 26 日 18:24 UTC
- 编辑时间：2023 年 3 月 26 日 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZonePreviewConsoleFullAccess

描述：DataZone 通过提供对 Amazon 预览版的完全访问权限 AWS Management Console。还提供对其他相关服务的部分访问权限。

AmazonDataZonePreviewConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZonePreviewConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 28 日 15:16 UTC
- 编辑时间：2023 年 7 月 13 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

描述：Amazon DataZone 创建用于部署数据分析项目的 IAM 角色。DataZone 在创建这些角色时使用此策略来定义其权限边界。

AmazonDataZoneProjectDeploymentPermissionsBoundary 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneProjectDeploymentPermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 21 日 02:54 UTC
- 编辑时间：2023 年 4 月 4 日 02:48 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneProjectDeploymentPermissionsBoundary

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
  "*"
]
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneProjectRolePermissionsBoundary

描述：Amazon 为项目 DataZone 创建 IAM 角色以执行数据分析操作，并在创建这些角色时使用此策略来定义其权限边界。

AmazonDataZoneProjectRolePermissionsBoundary 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneProjectRolePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 21 日 02:51 UTC
- 编辑时间：2023 年 3 月 21 日 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*",
    "datzone:*"
  ],
  "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",
"iam:*",
"redshift:*",
"redshift-data:*",
"tag:GetResources",
"iam:List*",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:PassRole",
"sqlworkbench:*",
"datazone:*"
],
"Resource" : [
```

```
        "*"
    ]
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

描述：Amazon DataZone 是一项数据管理服务，可让您对数据进行分类、发现、管理、共享和分析。借助 Amazon DataZone，您可以跨账户和支持的地区共享和访问您的数据。亚马逊 DataZone 简化了您的跨 AWS 服务体验，包括但不限于亚马逊 Redshift、Amazon Athena、Glue 和 Lake Formation。

AWS AWS

AmazonDataZoneRedshiftGlueProvisioningPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneRedshiftGlueProvisioningPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 22 日 20:19 UTC
- 编辑时间：世界标准时间 2024 年 3 月 12 日 16:44
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ],
    "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*"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

描述：此策略允许亚马逊将亚马逊 DataZone Redshift 数据发布到目录中。它还允许亚马逊授予访问 DataZone 权限或撤销对目录中已发布的亚马逊 Redshift 或 Amazon Redshift Serverless 资源的访问权限或撤消访问权限。

AmazonDataZoneRedshiftManageAccessRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneRedshiftManageAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 22 日 20:15 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 22:04
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "getNamespacePermission",
  "Effect" : "Allow",
  "Action" : "redshift-serverless:GetNamespace",
  "Resource" : [
    "arn:aws:redshift-serverless:*:*:namespace/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}

```

```
    },
    {
      "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*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

描述：该 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 策略是允许对在 Amazon DataZone 配置的 SageMaker 环境中创建的执行角色的权限列表。

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 23 日 23:01
- 编辑时间：世界标准时间 2024 年 5 月 8 日 02:03
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AllowAddTagsForAppAndSpace",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:app/*",
    "arn:aws:sagemaker:*:*:space/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "sagemaker:TaggingAction" : [
        "CreateApp",
        "CreateSpace"
      ]
    }
  }
}
```

```
    },
    {
      "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

描述：该 AmazonDataZoneSageMakerManageAccessRolePolicy 策略授予 Amazon DataZone 授予用户访问 SageMaker 环境中各种资源所需的权限。

AmazonDataZoneSageMakerManageAccessRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneSageMakerManageAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 23 日 23:34
- 编辑时间：世界标准时间 2024 年 4 月 23 日 23:34
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerManageAccessRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
},
{
  "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*"
  ]
},
{
```



```
"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"  
      ]  
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

描述：该 AmazonDataZoneSageMakerProvisioningRolePolicy 政策授予亚马逊 DataZone 与亚马逊 SageMaker 互操作所需的权限。

AmazonDataZoneSageMakerProvisioningRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDataZoneSageMakerProvisioningRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 23 日 23:32
- 编辑时间：世界标准时间 2024 年 4 月 23 日 23:32
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerProvisioningRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ],
    "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDetectiveFullAccess

描述：提供对 Amazon Detective 服务的完全访问权限和对控制台用户界面依赖项的限定访问权限

AmazonDetectiveFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDetectiveFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 30 日 17:57 UTC
- 编辑时间：2023 年 5 月 17 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDetectiveInvestigatorAccess

描述：为调查人员提供对 Amazon Detective 服务的访问权限以及对控制台 UI 依赖项的限定访问权限。该策略允许出于调查目的深入探究 Detective，并允许对 Guardduty 的有限写入权限。

AmazonDetectiveInvestigatorAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDetectiveInvestigatorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 1 月 17 日 15:24 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 03:13
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDetectiveMemberAccess

描述：为成员提供对 Amazon Detective 服务的访问权限以及对控制台用户界面依赖项的限定访问权限。

AmazonDetectiveMemberAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDetectiveMemberAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 17 日 15:16 UTC
- 编辑时间：2023 年 1 月 17 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDetectiveOrganizationsAccess

描述：为 Organizations 提供管理 Amazon Detective 的委托管理员的权限以及对控制台用户界面依赖项的限定访问权限。此策略还授予为 Detective 创建服务相关角色的权限。

AmazonDetectiveOrganizationsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDetectiveOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 2 日 15:20 UTC
- 编辑时间：2023 年 3 月 2 日 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDetectiveServiceLinkedRolePolicy

描述：允许 Amazon Detective 代表你拨打服务电话

AmazonDetectiveServiceLinkedRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 18 日 19:47 UTC
- 编辑时间：2021 年 11 月 18 日 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDevOpsGuruConsoleFullAccess

描述：该策略授予对 DevOps Guru 控制台的完全访问权限。

AmazonDevOpsGuruConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDevOpsGuruConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 12 月 17 日 18:43 UTC
- 编辑时间：2022 年 8 月 25 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDevOpsGuruFullAccess

描述：提供对 Amazon DevOps Guru 的完全访问权限。

AmazonDevOpsGuruFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDevOpsGuruFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:38 UTC
- 编辑时间：2022 年 8 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
    }
  }
}
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDevOpsGuruOrganizationsAccess

描述：提供在组织内启用和管理 Amazon DevOps Guru 的权限。

AmazonDevOpsGuruOrganizationsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDevOpsGuruOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 15 日 23:50 UTC
- 编辑时间：2021 年 11 月 15 日 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```



```
    }  
  ]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDevOpsGuruReadOnlyAccess

描述：提供对 Amazon DevOps Guru 控制台的只读访问权限。

AmazonDevOpsGuruReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDevOpsGuruReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:34 UTC
- 编辑时间：2022 年 8 月 25 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDevOpsGuruServiceRolePolicy

描述：Amazon DevOpsGuru 访问您的资源所需的服务相关角色。

AmazonDevOpsGuruServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 1 日 10:24 UTC
- 编辑时间：2023 年 1 月 10 日 14:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDMSCloudWatchLogsRole

描述：提供将 DMS 复制日志上传到客户账户中的 cloudwatch 日志的权限。

AmazonDMSCloudWatchLogsRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDMSCloudWatchLogsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 7 日 23:44 UTC
- 编辑时间：2023 年 5 月 23 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDMSRedshiftS3Role

描述：提供管理 DMS 的 Redshift 端点的 S3 设置的权限。

AmazonDMSRedshiftS3Role 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDMSRedshiftS3Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 4 月 20 日 17:05 UTC
- 编辑时间：2019 年 7 月 8 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDMSVPCManagementRole

描述：提供管理 AWS 托管客户配置的 VPC 设置的权限

AmazonDMSVPCManagementRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDMSVPCManagementRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2015 年 11 月 18 日 16:33 UTC
- 编辑时间：2016 年 5 月 23 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDB-ElasticServiceRolePolicy

描述：允许亚马逊 DocumentDB-Elastic 代表您管理 AWS 资源。

AmazonDocDB-ElasticServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型：**服务相关角色策略
- **创建日期：**2022 年 11 月 30 日 14:17 UTC
- **编辑时间：**2022 年 11 月 30 日 14:17 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
        ]
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDBConsoleFullAccess

描述：提供使用管理兼容 MongoDB 的 Amazon DocumentDB 的完全访问权限。AWS Management Console 请注意，该策略还授予向账户内的所有 SNS 主题发布的完全访问权限、创建和编辑 Amazon EC2 实例和 VPC 配置的权限、在 Amazon KMS 上查看和列出密钥的权限，以及对 Amazon RDS 和 Amazon Neptune 的完全访问权限。

AmazonDocDBConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDocDBConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 9 日 20:37 UTC
- 编辑时间：2022 年 11 月 30 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDBElasticFullAccess

描述：提供对 Amazon DocumentDB 弹性集群的完全访问权限以及其他必需权限，包括 EC2 SecretsManager、KMS CloudWatch 和 IAM。

AmazonDocDBElasticFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDocDBElasticFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 5 日 13:51 UTC
- 编辑时间：2023 年 6 月 21 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "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"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "docdb-elastic.*.amazonaws.com"
      ],
      "aws:ResourceTag/DocDBElasticFullAccess" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/DocDBElasticFullAccess" : "*",
      "kms:ViaService" : [
        "docdb-elastic.*.amazonaws.com"
      ]
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:GetResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
    },
    "StringEquals" : {
      "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDBElasticReadOnlyAccess

描述：提供对 Amazon Docdb-Elastic 和指标的只读访问权限。 CloudWatch

AmazonDocDBElasticReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDocDBElasticReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 8 日 14:37 UTC
- 编辑时间：2023 年 6 月 21 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDBFullAccess

描述：提供对亚马逊文档数据库的完全访问权限，兼容 MongoDB。请注意，该策略还授予向账户内的所有 SNS 主题发布的完全访问权限，以及对 Amazon RDS 和 Amazon Neptune 的完全访问权限。

AmazonDocDBFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDocDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 9 日 20:21 UTC
- 编辑时间：2019 年 1 月 9 日 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:RemoveTagsForResource",
"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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDocDBReadOnlyAccess

描述：提供对兼容 MongoDB 的亚马逊文档数据库的只读访问权限。请注意，该策略还授予对 Amazon RDS 和 Amazon Neptune 资源的访问权限。

AmazonDocDBReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDocDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 9 日 20:30 UTC
- 编辑时间：2019 年 1 月 9 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDRSVPCManagement

描述：提供管理 Amazon 托管客户配置的 VPC 设置的权限

AmazonDRSVPCManagement 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDRSVPCManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 9 月 2 日 00:09 UTC
- 编辑时间：2015 年 9 月 2 日 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDynamoDBFullAccess

描述：通过提供对亚马逊 DynamoDB 的完全访问权限。AWS Management Console

AmazonDynamoDBFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDynamoDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2021 年 1 月 29 日 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDynamoDBFullAccesswithDataPipeline

描述：此政策已进入弃用路径。有关指南，请参阅文档：<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>。提供对 Amazon DynamoDB 的完全访问权限，包括通过 Data Pipelin AWS e 进行导出/导入。AWS Management Console

AmazonDynamoDBFullAccesswithDataPipeline是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonDynamoDBFullAccesswithDataPipeline 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 11 月 12 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDynamoDBReadOnlyAccess

描述：通过提供对亚马逊 DynamoDB 的只读访问权限。AWS Management Console

AmazonDynamoDBReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonDynamoDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 3 月 20 日 15:45
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEBSCSIDriverPolicy

描述：允许 CSI 驱动程序服务账户代表您调用 EC2 等相关服务的 IAM 政策。

AmazonEBSCSIDriverPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEBSCSIDriverPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 4 日 17:24 UTC
- 编辑时间：2022 年 11 月 18 日 14:42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Action" : [
  "ec2:CreateSnapshot",
  "ec2:AttachVolume",
  "ec2:DetachVolume",
  "ec2:ModifyVolume",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeInstances",
  "ec2:DescribeSnapshots",
  "ec2:DescribeTags",
  "ec2:DescribeVolumes",
  "ec2:DescribeVolumesModifications"
],
"Resource" : "*"
},
{
  "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" : "*",
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/CSIVolumeName" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/CSIVolumeName" : "*"
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVolume"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerRegistryFullAccess

描述：提供对 Amazon ECR 资源的管理访问权限

AmazonEC2ContainerRegistryFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 21 日 17:06 UTC
- 编辑时间：2020 年 12 月 5 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerRegistryPowerUser

描述：提供对 Amazon EC2 容器注册表存储库的完全访问权限，但不允许删除存储库或更改策略。

AmazonEC2ContainerRegistryPowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerRegistryPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 21 日 17:05 UTC
- 编辑时间：2019 年 12 月 10 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ],
  "Resource" : "*"
}
```



```
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerRegistryReadOnly

描述：提供对 Amazon EC2 容器注册表存储库的只读访问权限。

AmazonEC2ContainerRegistryReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerRegistryReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 21 日 17:04 UTC
- 编辑时间：2019 年 12 月 10 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerServiceAutoscaleRole

描述：为 Amazon EC2 Container Service 启用任务自动扩展功能的策略

AmazonEC2ContainerServiceAutoscaleRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerServiceAutoscaleRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 5 月 12 日 23:25 UTC
- 编辑时间：2018 年 2 月 5 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerServiceEventsRole

描述：为 EC2 容器服务启用 CloudWatch 事件的策略

AmazonEC2ContainerServiceEventsRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerServiceEventsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 5 月 30 日 16:51 UTC
- 编辑时间：2023 年 3 月 6 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerServiceforEC2Role

描述：亚马逊 EC2 容器服务 Amazon EC2 角色的默认策略。

AmazonEC2ContainerServiceforEC2Role 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerServiceforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 3 月 19 日 18:45 UTC
- 编辑时间：2023 年 3 月 6 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ContainerServiceRole

描述：Amazon ECS 服务角色的默认策略。

AmazonEC2ContainerServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ContainerServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 16:14 UTC
- 编辑时间：2016 年 8 月 11 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ]
    }
  ]
}
```



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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2FullAccess

描述：通过提供对 Amazon EC2 的完全访问权限 AWS Management Console。

AmazonEC2FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 11 月 27 日 02:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2ReadOnlyAccess

描述：通过提供对 Amazon EC2 的只读访问权限 AWS Management Console。

AmazonEC2ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 18:43
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "ec2:Describe*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:Describe*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:Describe*",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RoleforAWSCodeDeploy

描述：提供 EC2 对 S3 存储桶的访问权限以下载修订版。EC2 实例上的 CodeDeploy 代理需要此角色。

AmazonEC2RoleforAWSCodeDeploy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2RoleforAWSCodeDeploy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 19 日 18:10 UTC
- 编辑时间：2017 年 3 月 20 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RoleforAWSCodeDeployLimited

描述：为 EC2 提供对 S3 存储桶的有限访问权限以下载修订版。EC2 实例上的 CodeDeploy 代理需要此角色。

AmazonEC2RoleforAWSCodeDeployLimited是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2RoleforAWSCodeDeployLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 24 日 17:55 UTC
- 编辑时间：2022 年 1 月 20 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RoleforDataPipelineRole

描述：适用于 Data Pipeline 的 Amazon EC2 角色服务角色的默认策略。

AmazonEC2RoleforDataPipelineRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2RoleforDataPipelineRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2016 年 2 月 22 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
```



```
        "*"
    ]
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RoleforSSM

描述：此政策将很快被弃用。请使用 AmazonSSM ManagedInstanceCore 政策在 EC2 实例上启用 S AWS systems Manager 服务核心功能。欲了解更多信息，请参阅 <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

AmazonEC2RoleforSSM是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2RoleforSSM 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 29 日 17:48 UTC
- 编辑时间：2019 年 1 月 24 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RolePolicyForLaunchWizard

描述：适用于 EC2 的 Amazon LaunchWizard 服务角色的托管策略

AmazonEC2RolePolicyForLaunchWizard 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2RolePolicyForLaunchWizard 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 08:05 UTC
- 编辑时间：2022 年 5 月 16 日 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

策略版本

策略版本：v10（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems",
      "fsx:ListTagsForResource",
      "fsx:DescribeStorageVirtualMachines"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : "LaunchWizard*"
      }
    }
  }
]
```


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2SpotFleetAutoscaleRole

描述：为 Amazon EC2 竞价队列启用自动扩缩功能的策略

AmazonEC2SpotFleetAutoscaleRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2SpotFleetAutoscaleRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 8 月 19 日 18:27 UTC
- 编辑时间：2019 年 2 月 18 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2SpotFleetTaggingRole

描述：允许 EC2 Spot 队列代表您请求、终止和标记竞价型实例。

AmazonEC2SpotFleetTaggingRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEC2SpotFleetTaggingRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 6 月 29 日 18:19 UTC
- 编辑时间：2020 年 4 月 23 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonECS_FullAccess

描述：提供对 Amazon ECS 资源的管理访问权限，并通过访问其他 AWS 服务资源（包括 VPC、Auto Scaling 组和 CloudFormation 堆栈）来启用 ECS 功能。

AmazonECS_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonECS_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 7 日 21:36 UTC
- 编辑时间：2023 年 1 月 4 日 16:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

策略版本

策略版本：v20（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"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" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter",
    "ssm:GetParameters",
    "ssm:GetParametersByPath"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteInternetGateway",
    "ec2>DeleteRoute",

```



```
    "ec2:DeleteRouteTable",
    "ec2:DeleteSecurityGroup"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ecs-tasks.amazonaws.com"
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/ecsInstanceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/ecsAutoscaleRole*"
  ]
}
```

```
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "application-autoscaling.amazonaws.com",
          "application-autoscaling.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "ecs.amazonaws.com",
          "ecs.application-autoscaling.amazonaws.com",
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticloadbalancing:CreateAction" : [
          "CreateTargetGroup",
          "CreateRule",
          "CreateListener",
          "CreateLoadBalancer"
        ]
      }
    }
  }
]
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

描述：提供对私有证书颁发机构、S AWS secrets Manager 以及代表您管理 ECS Service Connect TLS 功能 AWS 服务 所需的其他功能的管理权限。

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 是一个 [AWS 托管策略](#)。

使用此策略

您可以将

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 19 日 20:08
- 编辑时间：世界标准时间 2024 年 1 月 19 日 20:08
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonECSInfrastructureRolePolicyForVolumes

描述：提供代表您管理与 ECS 工作负载关联的卷所需的其他 AWS 服务资源的访问权限。

AmazonECSInfrastructureRolePolicyForVolumes 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonECSInfrastructureRolePolicyForVolumes 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 10 日 22:56
- 编辑时间：世界标准时间 2024 年 1 月 10 日 22:56
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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" : "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/AmazonECSManaged" : "arn:aws:ecs:*:*:task/*"
    },
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonECSServiceRolePolicy

描述：允许 Amazon ECS 管理您的集群的策略。

AmazonECSServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 14 日 01:18 UTC
- 编辑时间：世界标准时间 2023 年 12 月 4 日 19:32
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonECSTaskExecutionRolePolicy

描述：提供对运行 Amazon ECS 任务所需的其他 AWS 服务资源的访问权限

AmazonECSTaskExecutionRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonECSTaskExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 16 日 18:48 UTC
- 编辑时间：2017 年 11 月 16 日 18:48 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEFSCSIDriverPolicy

描述：提供对 EFS 资源的管理访问权限和 EC2 的读取权限

AmazonEFSCSIDriverPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEFSCSIDriverPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 7 月 25 日 20:10 UTC
- 编辑时间：2023 年 7 月 25 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKS_CNI_Policy

描述：此策略为 Amazon VPC CNI 插件 (amazon-vpc-cni-k8s) 提供了修改您的 EKS 工作节点上的 IP 地址配置所需的权限。此权限集允许 CNI 代表您列出、描述和修改弹性网络接口。有关 AWS VPC CNI 插件的更多信息，请点击此处：<https://github.com/aws/8s-amazon-vpc-cni-k>

AmazonEKS_CNI_Policy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKS_CNI_Policy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 27 日 21:07 UTC
- 编辑时间：世界标准时间 2024 年 3 月 4 日 20:20
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSClusterPolicy

描述：此策略为 Kubernetes 提供了代表您管理资源所需的权限。Kubernetes 需要 Ec2: CreateTags 权限才能在 EC2 资源上放置识别信息，包括但不限于实例、安全组和弹性网络接口。

AmazonEKSClusterPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSClusterPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 27 日 21:06 UTC
- 编辑时间：2023 年 2 月 7 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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",
"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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSCoordinatorServiceRolePolicy

描述：此策略允许 Amazon EKS 管理 EKS 连接器的 AWS 资源

AmazonEKSCoordinatorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 4 日 20:31 UTC
- 编辑时间：2021 年 9 月 4 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSFargatePodExecutionRolePolicy

描述：提供对在 AWS Fargate 上运行 Amazon EKS 容器所需的其他 AWS 服务资源的访问权限

AmazonEKSFargatePodExecutionRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSFargatePodExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 22 日 04:34 UTC
- 编辑时间：2019 年 11 月 22 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSForFargateServiceRolePolicy

描述：此策略向 Amazon EKS 授予运行 fargate 任务所需的权限

AmazonEKSForFargateServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 22 日 04:36 UTC
- 编辑时间：2019 年 11 月 22 日 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSLocalOutpostClusterPolicy

描述：此策略为在您的账户中运行的 EKS 本地集群的控制平面实例提供代表您管理资源的权限。

AmazonEKSLocalOutpostClusterPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSLocalOutpostClusterPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 24 日 21:56 UTC
- 编辑时间：2022 年 10 月 17 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
```

```

    "ec2:DescribeTags",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeInstanceTypes",
    "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/*:*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSLocalOutpostServiceRolePolicy

描述：允许 Amazon EKS Local 代表您呼叫 AWS 服务。

AmazonEKSLocalOutpostServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 8 月 23 日 21:53 UTC
- 编辑时间：2022 年 10 月 24 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "ssm:ResumeSession",
    "ssm:TerminateSession"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "outposts:GetOutpost"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSServicePolicy

描述：此策略允许适用于 Kubernetes 的亚马逊弹性容器服务 Elastic Container Service 创建和管理运行 EKS 集群所需的资源。

AmazonEKSServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSServicePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 27 日 21:08 UTC
- 编辑时间：2020 年 5 月 27 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "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" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "eks.amazonaws.com"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSServiceRolePolicy

描述： Amazon EKS 代表您调用服务所需的 AWS 服务相关角色。

AmazonEKSServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 2 月 21 日 20:10 UTC

- 编辑时间：2020 年 5 月 27 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterfacePermission",
        "iam:ListAttachedRolePolicies",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2>DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```



```
    "ForAnyValue:StringLike" : {
      "ec2:ResourceTag/Name" : "eks-cluster-sg*"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:subnet/*"
    ],
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "kubernetes.io/cluster/*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : [
          "kubernetes.io/cluster/*"
        ],
        "aws:RequestTag/Name" : "eks-cluster-sg*"
      }
    }
  },
  {
    "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/*:*:*"
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSVPCResourceController

描述：VPC 资源控制器用于管理工作节点的 ENI 和 IP 的策略。

AmazonEKSVPCResourceController 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSVPCResourceController 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2020 年 8 月 12 日 00:55 UTC
- 编辑时间 : 2020 年 8 月 12 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSWorkerNodePolicy

描述：此策略允许 Amazon EKS 工作节点连接到 Amazon EKS 集群。

AmazonEKSWorkerNodePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEKSWorkerNodePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 27 日 21:09 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 00:06
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElastiCacheFullAccess

描述：提供 ElastiCache 通过 Amazon 的完全访问权限 AWS Management Console。

AmazonElastiCacheFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElastiCacheFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：世界标准时间 2023 年 11 月 28 日 03:49
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElastiCacheReadOnlyAccess

描述：ElastiCache 通过提供对 Amazon 的只读访问权限 AWS Management Console。

AmazonElastiCacheReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElastiCacheReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticCacheReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticContainerRegistryPublicFullAccess

描述：提供对 Amazon ECR 公共资源的管理访问权限

AmazonElasticContainerRegistryPublicFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticContainerRegistryPublicFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 17:25 UTC
- 编辑时间：2020 年 12 月 1 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticContainerRegistryPublicPowerUser

描述：提供对 Amazon ECR 公共存储库的完全访问权限，但不允许删除存储库或更改策略。

AmazonElasticContainerRegistryPublicPowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticContainerRegistryPublicPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:16 UTC
- 编辑时间：2020 年 12 月 1 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticContainerRegistryPublicReadOnly

描述：提供对 Amazon ECR 公共存储库的只读访问权限。

AmazonElasticContainerRegistryPublicReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticContainerRegistryPublicReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 17:27 UTC

- 编辑时间：2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemClientFullAccess

描述：提供对 Amazon EFS 文件系统的根客户端访问权限

AmazonElasticFileSystemClientFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemClientFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 13 日 16:27 UTC
- 编辑时间：2020 年 1 月 13 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemClientReadOnlyAccess

描述：提供对 Amazon EFS 文件系统的只读客户端访问权限

AmazonElasticFileSystemClientReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemClientReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 13 日 16:24 UTC
- 编辑时间：2020 年 1 月 13 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:ClientMount",
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemClientReadWriteAccess

描述：提供对 Amazon EFS 文件系统的读写客户端访问权限

AmazonElasticFileSystemClientReadWriteAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemClientReadWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 13 日 16:21 UTC
- 编辑时间：2020 年 1 月 13 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemFullAccess

描述：通过提供对 Amazon EFS 的完全访问权限 AWS Management Console。

AmazonElasticFileSystemFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 5 月 27 日 16:22 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 16:53
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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",
"kms:DescribeKey",
"kms:ListAliases"
],
"Sid" : "ElasticFileSystemFullAccess",
"Effect" : "Allow",
"Resource" : "*"
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Sid" : "CreateServiceLinkedRoleForEFS",
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "elasticfilesystem.amazonaws.com"
      ]
    }
  }
}
]
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemReadOnlyAccess

描述：通过提供对 Amazon EFS 的只读访问权限 AWS Management Console。

AmazonElasticFileSystemReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 27 日 16:25 UTC
- 编辑时间：2022 年 1 月 10 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "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",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemServiceRolePolicy

描述：允许 Amazon Elastic File System 代表您管理 AWS 资源

AmazonElasticFileSystemServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 5 日 16:52 UTC
- 编辑时间：2022 年 1 月 10 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticFileSystemsUtils

描述：允许客户使用 S AWS systems Manager 自动管理其 EC2 实例上的 Amazon EFS 实用程序 (amazon-efs-utils) 包，并用于 CloudWatchLog 获取 EFS 文件系统挂载成功/失败通知。

AmazonElasticFileSystemsUtils是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticFileSystemsUtils 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 29 日 15:16 UTC
- 编辑时间：2020 年 9 月 29 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"    
  }  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceEditorsRole

描述：Amazon Elastic Editor MapReduce s 服务角色的默认策略。

AmazonElasticMapReduceEditorsRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceEditorsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 16 日 21:55 UTC
- 编辑时间：2023 年 2 月 9 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceforAutoScalingRole

描述：适用于 Auto Scaling MapReduce 的亚马逊 Elastic。允许 Auto Scaling 向您的 EMR 集群中添加和从中删除实例的角色。

AmazonElasticMapReduceforAutoScalingRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceforAutoScalingRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 11 月 18 日 01:09 UTC
- 编辑时间：2016 年 11 月 18 日 01:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceforEC2Role

描述：适用于 EC2 的 Amazon Elastic 服务角色 MapReduce 的默认策略。

AmazonElasticMapReduceforEC2Role 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2017 年 8 月 11 日 23:57 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceFullAccess

描述：此政策已进入弃用路径。有关指导，请参阅文档：<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。提供对 Amazon Elastic MapReduce 及其所需的底层服务（例如 EC2 和 S3）的完全访问权限

AmazonElasticMapReduceFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 10 月 11 日 15:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]

```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReducePlacementGroupPolicy

描述：允许 EMR 创建、描述和删除 EC2 置放群组的政策。

AmazonElasticMapReducePlacementGroupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReducePlacementGroupPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 29 日 00:37 UTC
- 编辑时间：2020 年 9 月 29 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceReadOnlyAccess

描述：通过提供对 Amazon Elastic MapReduce 的只读访问权限 AWS Management Console。

AmazonElasticMapReduceReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2020 年 7 月 29 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticMapReduceRole

描述：此策略已进入弃用路径。有关指导，请参阅文档：<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。Amazon 弹性 MapReduce 服务角色的默认策略。

AmazonElasticMapReduceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticMapReduceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2020 年 6 月 24 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticsearchServiceRolePolicy

描述：允许 Amazon Elasticsearch Service 代表您访问其他 AWS 服务，例如 EC2 联网 API。

AmazonElasticsearchServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 7 月 7 日 00:15 UTC
- 编辑时间：2023 年 10 月 23 日 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticTranscoder_FullAccess

描述：向用户授予对 Elastic Transcoder 的完全访问权限以及访问完整的 Elastic Transcoder 功能所需的相关服务的权限。

AmazonElasticTranscoder_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticTranscoder_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 27 日 18:59 UTC
- 编辑时间：2019 年 6 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticTranscoder_JobsSubmitter

描述：授予用户更改预设、提交作业和查看 Elastic Transcoder 设置的权限。此策略还授予使用 Elastic Transcoder 控制台所需的某些其他服务的某些只读访问权限，包括 S3、IAM 和 SNS。

AmazonElasticTranscoder_JobsSubmitter 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticTranscoder_JobsSubmitter 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 7 日 21:12 UTC
- 编辑时间：2019 年 6 月 10 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticTranscoder_ReadOnlyAccess

描述：授予用户对 Elastic Transcoder 的只读访问权限和对相关服务的列表访问权限。

AmazonElasticTranscoder_ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticTranscoder_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 7 日 21:09 UTC
- 编辑时间：2019 年 6 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonElasticTranscoderRole

描述：亚马逊 Elastic Transcoder 服务角色的默认策略。

AmazonElasticTranscoderRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonElasticTranscoderRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2019 年 6 月 13 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRCleanupPolicy

描述：允许 EMR 服务角色在 EMR 服务角色失去该能力时执行终止和删除 AWS EC2 资源所需的操作。

AmazonEMRCleanupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 26 日 23:54 UTC
- 编辑时间：2020 年 9 月 29 日 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRContainersServiceRolePolicy

描述：允许访问运行 Amazon EMR 所需的其他 AWS 服务资源

AmazonEMRContainersServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 9 日 00:38 UTC
- 编辑时间：2023 年 3 月 10 日 22:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

```
    ],
    "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRFullAccessPolicy_v2

描述：提供对 Amazon EMR 的完全访问权限

AmazonEMRFullAccessPolicy_v2是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEMRFullAccessPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 12 日 01:50 UTC
- 编辑时间：2023 年 7 月 28 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:CreateSecurityConfiguration",
"elasticmapreduce>DeleteEditor",
"elasticmapreduce>DeleteSecurityConfiguration",
"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: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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRReadOnlyAccessPolicy_v2

描述：提供对 Amazon EMR 和相关 CloudWatch 指标的只读访问权限。

AmazonEMRReadOnlyAccessPolicy_v2是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEMRReadOnlyAccessPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 12 日 01:39 UTC
- 编辑时间：2023 年 8 月 2 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRServerlessServiceRolePolicy

描述：允许访问运行 Amazon emrServerLess 所需的其他 AWS 服务资源

AmazonEMRServerlessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 5 月 20 日 23:15 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 18:21
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEMRServicePolicy_v2

描述：此策略用于 Amazon EMR 服务角色，不应用于您账户中的任何其他 IAM 用户或角色。此策略授予创建和管理 EMR 相关资源以及运行 EMR 集群所需的相关服务的权限。

AmazonEMRServicePolicy_v2是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEMRServicePolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 3 月 12 日 01:11 UTC

- 编辑时间：世界标准时间 2024 年 5 月 2 日 18:43
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonESCognitoAccess

描述：提供对 Amazon Cognito 配置服务的有限访问权限。

AmazonESCognitoAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonESCognitoAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 28 日 22:29 UTC
- 编辑时间：2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonESFullAccess

描述：提供对 Amazon ES 配置服务的完全访问权限。

AmazonESFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonESFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 1 日 19:14 UTC
- 编辑时间：2015 年 10 月 1 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonESReadOnlyAccess

描述：提供对 Amazon ES 配置服务的只读访问权限。

AmazonESReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonESReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 1 日 19:18 UTC
- 编辑时间：2018 年 10 月 3 日 03:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

描述：EventBridge 允许代表您访问密钥管理器资源。

AmazonEventBridgeApiDestinationsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 2 月 11 日 20:52 UTC
- 编辑时间：2021 年 2 月 11 日 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeFullAccess

描述：提供对 Amazon 的完全访问权限 EventBridge。

AmazonEventBridgeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 11 日 14:08 UTC
- 编辑时间：2022 年 12 月 1 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "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"
    }
  }
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgePipesFullAccess

描述：提供对 Amazon Pip EventBridge es 的完全访问权限。

AmazonEventBridgePipesFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgePipesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 12 月 1 日 17:03 UTC
- 编辑时间：2022 年 12 月 1 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgePipesOperatorAccess

描述：提供对 Amazon Pipes 的只读权限和操作员（能够停止和开始运行 EventBridge 管道）。

AmazonEventBridgePipesOperatorAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgePipesOperatorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 12 月 1 日 17:04 UTC
- 编辑时间：2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgePipesReadOnlyAccess

描述：提供对 Amazon EventBridge Pipes 的只读访问权限。

AmazonEventBridgePipesReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgePipesReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 12 月 1 日 17:04 UTC
- 编辑时间：2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ]
    }
  ]
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeReadOnlyAccess

描述：提供对 Amazon 的只读访问权限 EventBridge。

AmazonEventBridgeReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 11 日 13:59 UTC
- 编辑时间：2022 年 12 月 1 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeSchedulerFullAccess

描述：AmazonEventBridgeSchedulerFullAccess 托管策略授予对计划和 EventBridge 计划组使用所有计划程序操作的权限。

AmazonEventBridgeSchedulerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeSchedulerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 18:37 UTC
- 编辑时间：2022 年 11 月 10 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeSchedulerReadOnlyAccess

描述： AmazonEventBridgeSchedulerReadOnlyAccess 托管策略授予只读权限，以查看有关您的日程安排和计划组的详细信息。

AmazonEventBridgeSchedulerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeSchedulerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 18:50 UTC
- 编辑时间：2022 年 11 月 10 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ]
    }
  ]
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeSchemasFullAccess

描述：提供对 Amazon EventBridge 架构的完全访问权限。

AmazonEventBridgeSchemasFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeSchemasFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 28 日 23:12 UTC
- 编辑时间：2019 年 11 月 28 日 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeSchemasReadOnlyAccess

描述：提供对 Amazon EventBridge 架构的只读访问权限。

AmazonEventBridgeSchemasReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonEventBridgeSchemasReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 28 日 23:05 UTC
- 编辑时间：2020 年 5 月 1 日 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEventBridgeSchemasServiceRolePolicy

描述：向由 Amazon EventBridge 架构创建的托管规则授予权限。

AmazonEventBridgeSchemasServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 27 日 01:10 UTC
- 编辑时间：2019 年 11 月 27 日 01:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFISServiceRolePolicy

描述：允许 AWS FIS 管理实验的监控和资源选择的策略。

AmazonFISServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 21 日 21:18 UTC
- 编辑时间：2022 年 10 月 25 日 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonForecastFullAccess

描述：允许访问 Amazon Forecast 的所有操作

AmazonForecastFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonForecastFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 01:52 UTC
- 编辑时间：2019 年 1 月 18 日 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "forecast:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "forecast.amazonaws.com"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFraudDetectorFullAccessPolicy

描述：允许访问 Amazon Fraud Detector 的所有操作

AmazonFraudDetectorFullAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFraudDetectorFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 22:46 UTC
- 编辑时间：2019 年 12 月 3 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFreeRTOSFullAccess

描述：亚马逊 FreeRTOS 的完全访问政策

AmazonFreeRTOSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFreeRTOSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 15:32 UTC
- 编辑时间：2017 年 11 月 29 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFreeRTOSOTAUpdate

描述：允许用户访问亚马逊 FreeRTOS OTA 更新

AmazonFreeRTOSOTAUpdate 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFreeRTOSOTAUpdate 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 8 月 27 日 22:43 UTC
- 编辑时间：2020 年 12 月 18 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFSxConsoleFullAccess

描述：提供对 Amazon FSx 的完全访问权限和通过访问相关 AWS 服务的权限。AWS Management Console

AmazonFSxConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFSxConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:36 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:07
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Sid" : "ListResourcesAssociatedWithFSxFileSystem",
"Effect" : "Allow",
"Action" : [
  "cloudwatch:DescribeAlarms",
  "cloudwatch:GetMetricData",
  "ds:DescribeDirectories",
  "ec2:DescribeNetworkInterfaceAttribute",
  "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>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: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" : "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"
    ]
}
}
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFSxConsoleReadOnlyAccess

描述：提供对 Amazon FSx 的只读访问权限和通过访问相关 AWS 服务的权限。AWS Management Console

AmazonFSxConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFSxConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:35 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:19
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFSxFullAccess

描述：提供对 Amazon FSx 的完全访问权限和对相关 AWS 服务的访问权限。

AmazonFSxFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFSxFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:34 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:16
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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: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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFSxReadOnlyAccess

描述：提供对 Amazon FSx 的只读访问权限。

AmazonFSxReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonFSxReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:33 UTC
- 编辑时间：2018 年 11 月 28 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonFSxServiceRolePolicy

描述：允许 Amazon FSx 代表您管理 AWS 资源

AmazonFSxServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 28 日 10:38 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGlacierFullAccess

描述：提供通过 Amazon Glacier 的完全访问权限 AWS Management Console。

AmazonGlacierFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGlacierFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGlacierReadOnlyAccess

描述：通过提供对 Amazon Glacier 的只读访问权限 AWS Management Console。

AmazonGlacierReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGlacierReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2016 年 5 月 5 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGrafanaAthenaAccess

描述：该策略授予访问亚马逊 Athena 以及通过亚马逊 Grafana 中的亚马逊 Athena 插件查询和将结果写入 s3 所需的依赖项的权限。

AmazonGrafanaAthenaAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGrafanaAthenaAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 22 日 17:11 UTC
- 编辑时间：2021 年 11 月 22 日 17:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGrafanaCloudWatchAccess

描述：该政策授予访问亚马逊的权限 CloudWatch 以及 CloudWatch 用作亚马逊托管 Grafana 中的数据源所需的依赖项。

AmazonGrafanaCloudWatchAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGrafanaCloudWatchAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 3 月 24 日 22:41 UTC
- 编辑时间：2023 年 3 月 24 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGrafanaRedshiftAccess

描述：该政策授予对亚马逊 Redshift 的限定访问权限以及在 Amazon Grafana 中使用亚马逊 Redshift 插件所需的依赖项。

AmazonGrafanaRedshiftAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGrafanaRedshiftAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 26 日 23:15 UTC
- 编辑时间：2021 年 11 月 26 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGrafanaServiceLinkedRolePolicy

描述：提供对 Amazon Grafana 管理或使用的 AWS 资源的访问权限。

AmazonGrafanaServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 8 日 23:10 UTC
- 编辑时间：2022 年 11 月 8 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGuardDutyFullAccess

描述：提供使用 Amazon 的完全访问权限 GuardDuty。

AmazonGuardDutyFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGuardDutyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 22:31 UTC
- 编辑时间：世界标准时间 2024 年 6 月 10 日 22:50
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
}

```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

描述：GuardDuty 恶意软件防护使用名为的服务关联角色 (SLR)。

AWSServiceRoleForAmazonGuardDutyMalwareProtection 此服务相关角色允许 GuardDuty 恶意软件防护执行无代理扫描以检测恶意软件。它 GuardDuty 允许在您的帐户中创建快照，并与 GuardDuty 服务帐户共享快照以扫描恶意软件。它会评估这些共享快照，并将检索到的 EC2 实例元数据包含在 GuardDuty 恶意软件防护结果中。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服务相关角色信任恶意软件保护.guardduty.amazonaws.com 服务来代替该角色。

AmazonGuardDutyMalwareProtectionServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 19 日 19:06 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 22:24
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
}
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGuardDutyReadOnlyAccess

描述：提供对 Amazon GuardDuty 资源的只读访问权限

AmazonGuardDutyReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonGuardDutyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 22:29 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 23:07
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonGuardDutyServiceRolePolicy

描述：允许访问由 Amazon Guard Duty 使用或管理的 AWS 资源

AmazonGuardDutyServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 28 日 20:12 UTC
- 编辑时间：世界标准时间 2024 年 3 月 27 日 00:58
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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" : "*"
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHealthLakeFullAccess

描述：提供对 Amazon HealthLake 服务的完全访问权限。

AmazonHealthLakeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHealthLakeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 01:07 UTC
- 编辑时间：2021 年 2 月 17 日 01:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHealthLakeReadOnlyAccess

描述：提供对 Amazon HealthLake 服务的只读访问权限。

AmazonHealthLakeReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHealthLakeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 02:43 UTC
- 编辑时间：2021 年 2 月 17 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeFullAccess

描述：提供通过 AWS Management Console 和软件开发工具包对 Honeycode 的完全访问权限。

AmazonHoneycodeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeReadOnlyAccess

描述：通过 AWS Management Console 和 SDK 提供对 Honeycode 的只读访问权限。

AmazonHoneycodeReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeServiceRolePolicy

描述：Amazon Honeycode 访问您的资源所需的服务相关角色。

AmazonHoneycodeServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 18 日 18:03 UTC
- 编辑时间：2020 年 11 月 18 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeTeamAssociationFullAccess

描述：通过 AWS Management Console 和 SDK 提供对 Honeycode 团队协会的完全访问权限。

AmazonHoneycodeTeamAssociationFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeTeamAssociationFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

描述：通过 AWS Management Console 和 SDK 提供对 Honeycode 团队协会的只读访问权限。

AmazonHoneycodeTeamAssociationReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeTeamAssociationReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2020 年 6 月 24 日 20:27 UTC
- 编辑时间：2020 年 6 月 24 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeWorkbookFullAccess

描述：提供通过 AWS Management Console 和 SDK 对 Honeycode 工作簿的完全访问权限。

AmazonHoneycodeWorkbookFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeWorkbookFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHoneycodeWorkbookReadOnlyAccess

描述：通过 AWS Management Console 和 SDK 提供对 Honeycode 工作簿的只读访问权限。

AmazonHoneycodeWorkbookReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonHoneycodeWorkbookReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "honeycode:GetScreenData",
      "honeycode:DescribeTableDataImportJob",
      "honeycode:ListTableColumns",
      "honeycode:ListTableRows",
      "honeycode:ListTables",
      "honeycode:QueryTableRows"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspector2AgentlessServiceRolePolicy

描述：向 Amazon Inspector 授予执行无代理安全评估 AWS 服务 所需的访问权限

AmazonInspector2AgentlessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 20 日 15:18
- 编辑时间：世界标准时间 2023 年 11 月 20 日 15:18

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspector2FullAccess

描述：提供对 Amazon Inspector 的完全访问权限以及对其他相关服务（例如组织）的访问权限。

AmazonInspector2FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonInspector2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 19:10 UTC
- 编辑时间：世界标准时间 2024 年 4 月 25 日 13:21
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspector2ManagedCisPolicy

描述：这是一项托管策略，客户应将其附加到其角色上，以便与检查员服务部门进行通信以进行 CIS 扫描

AmazonInspector2ManagedCisPolicy是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonInspector2ManagedCisPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 1 月 24 日 16:31
- 编辑时间：世界标准时间 2024 年 1 月 24 日 16:31
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspector2ReadOnlyAccess

描述：提供对 Amazon inspector2 服务和相关支持服务的只读访问权限

AmazonInspector2ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonInspector2ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 1 月 21 日 14:45 UTC
- 编辑时间：2023 年 9 月 22 日，20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspector2ServiceRolePolicy

描述：向 Amazon Inspector 授予执行安全评估 AWS 服务所需的访问权限

AmazonInspector2ServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 16 日 20:27 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 14:06
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy

策略版本

策略版本：v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "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: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",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GatherInventory",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "ssm>DeleteAssociation",
    "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" : "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspectorFullAccess

描述：提供对 Amazon Inspector 的完全访问权限。

AmazonInspectorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonInspectorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 17:08 UTC
- 编辑时间：2017 年 12 月 21 日，14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspectorReadOnlyAccess

描述：提供对 Amazon Inspector 的只读访问权限。

AmazonInspectorReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonInspectorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 17:08 UTC
- 编辑时间：2019 年 10 月 1 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonInspectorServiceRolePolicy

描述：向 Amazon Inspector 授予执行安全评估 AWS 服务 所需的访问权限

AmazonInspectorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 21 日 15:48 UTC
- 编辑时间：2020 年 9 月 11 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKendraFullAccess

描述：通过提供对 Amazon Kendra 的完全访问权限。AWS Management Console

AmazonKendraFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKendraFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:15 UTC
- 编辑时间：2019 年 12 月 3 日 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKendraReadOnlyAccess

描述：通过提供对 Amazon Kendra 的只读访问权限。AWS Management Console

AmazonKendraReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKendraReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:13 UTC
- 编辑时间：2021 年 5 月 27 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKeyspacesFullAccess

描述：提供对 Amazon Keyspaces 的完全访问权限

AmazonKeyspacesFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKeyspacesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 23 日 17:06 UTC
- 编辑时间：2023 年 10 月 3 日，19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "Ec2VpcReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKeyspacesReadOnlyAccess

描述：提供对 Amazon Keyspaces 的只读访问权限

AmazonKeyspacesReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKeyspacesReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 23 日 17:07 UTC
- 编辑时间：2022 年 7 月 7 日 14:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKeyspacesReadOnlyAccess_v2

描述：提供对 Amazon Keyspaces 和相关 AWS 服务的只读访问权限。

AmazonKeyspacesReadOnlyAccess_v2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKeyspacesReadOnlyAccess_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 12 日 17:01 UTC
- 编辑时间：2023 年 9 月 12 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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",
      "cloudwatch:GetMetricData",
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisAnalyticsFullAccess

描述：通过 AWS Management Console 提供对亚马逊 Kinesis Analytics 的完全访问权限。

AmazonKinesisAnalyticsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 9 月 21 日 19:01 UTC
- 编辑时间：2016 年 9 月 21 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisAnalyticsReadOnly

描述：通过 AWS Management Console 提供对亚马逊 Kinesis Analytics 的只读访问权限。

AmazonKinesisAnalyticsReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisAnalyticsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 9 月 21 日 18:16 UTC
- 编辑时间：2016 年 9 月 21 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisFirehoseFullAccess

描述：提供对所有亚马逊 Kinesis Firehose Delivery Streams 的完全访问权限。

AmazonKinesisFirehoseFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisFirehoseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 18:45 UTC
- 编辑时间：2015 年 10 月 7 日 18:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
"Statement" : [
  {
    "Action" : [
      "firehose:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisFirehoseReadOnlyAccess

描述：提供对所有亚马逊 Kinesis Firehose 传送流的只读访问权限。

AmazonKinesisFirehoseReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisFirehoseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 18:43 UTC
- 编辑时间：2015 年 10 月 7 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisFullAccess

描述：通过提供对所有直播的完全访问权限 AWS Management Console。

AmazonKinesisFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisReadOnlyAccess

描述：通过提供对所有直播的只读访问权限 AWS Management Console。

AmazonKinesisReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisVideoStreamsFullAccess

描述：提供通过 AWS Management Console Amazon Kinesis Video Streams 的完全访问权限。

AmazonKinesisVideoStreamsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisVideoStreamsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 1 日 23:27 UTC
- 编辑时间：2017 年 12 月 1 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonKinesisVideoStreamsReadOnlyAccess

描述：提供通过 AWS AWS Management Console Kinesis Video Streams 的只读访问权限。

AmazonKinesisVideoStreamsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonKinesisVideoStreamsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 1 日 23:14 UTC
- 编辑时间：2017 年 12 月 1 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:Describe*",
      "kinesisvideo:Get*",
      "kinesisvideo:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLaunchWizard_Fullaccess

描述：对 AWS Launch 向导和其他必需服务的完全访问权限。

AmazonLaunchWizard_Fullaccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLaunchWizard_Fullaccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 6 日 17:47 UTC
- 编辑时间：2023 年 2 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLaunchWizardFullAccessV2

描述：对 AWS Launch 向导和其他必需服务的完全访问权限。

AmazonLaunchWizardFullAccessV2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLaunchWizardFullAccessV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 1 日 17:14 UTC
- 编辑时间：2023 年 9 月 1 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexChannelsAccess

描述：此策略允许客户从频道调用 Lex 运行时

AmazonLexChannelsAccess 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2021 年 1 月 13 日 20:12 UTC
- 编辑时间：2021 年 1 月 13 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexFullAccess

描述：通过提供对 Amazon Lex 的完全访问权限 AWS Management Console。此外还提供创建 Lex 服务关联角色的权限，并授予 Lex 调用一组有限的 Lambda 函数的权限。

AmazonLexFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLexFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:20 UTC
- 编辑时间：世界标准时间 2024 年 4 月 16 日 20:06
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexReadOnly

描述：提供对 Amazon Lex 的只读访问权限。

AmazonLexReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLexReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:13 UTC
- 编辑时间：2024 年 5 月 13 日，世界标准时间 16:58
- ARN: arn:aws:iam::aws:policy/AmazonLexReadOnly

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexReplicationPolicy

描述：允许 Amazon Lex 代表您跨区域复制 Lex 资源。

AmazonLexReplicationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 1 月 31 日 23:29
- 编辑时间：世界标准时间 2024 年 3 月 8 日 17:11
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:DeleteResourcePolicy"
  ],
  "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"
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexRunBotsOnly

描述：提供对 Amazon Lex 对话式 API 的访问权限。

AmazonLexRunBotsOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLexRunBotsOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:06 UTC
- 编辑时间：2021 年 8 月 18 日 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexV2BotPolicy

描述：为 Lex V2 机器人提供代表您呼叫其他 AWS 服务的权限。

AmazonLexV2BotPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 1 月 13 日 20:10 UTC
- 编辑时间：2021 年 1 月 13 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutEquipmentFullAccess

描述：提供对亚马逊 Lookout for Equipment 操作的完全访问权限

AmazonLookoutEquipmentFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutEquipmentFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 8 日 15:52 UTC
- 编辑时间：2021 年 11 月 24 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutEquipmentReadOnlyAccess

描述：提供对 Amazon Lookout for Equipments 的只读权限

AmazonLookoutEquipmentReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutEquipmentReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 5 日 16:47 UTC
- 编辑时间：2022 年 11 月 10 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutMetricsFullAccess

描述：允许访问亚马逊 Lookout for Metrics 的所有操作

AmazonLookoutMetricsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutMetricsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 7 日 00:43 UTC
- 编辑时间：2021 年 5 月 7 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutMetricsReadOnlyAccess

描述：允许访问 Amazon Lookout for Metrics 的所有只读操作

AmazonLookoutMetricsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutMetricsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 7 日 00:43 UTC
- 编辑时间：2022 年 1 月 4 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutVisionConsoleFullAccess

描述：提供对 Amazon Lookout for Vision 的完全访问权限，以及对所需服务和控制台依赖项的限定访问权限。

AmazonLookoutVisionConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutVisionConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 11 日 19:37 UTC
- 编辑时间：2021 年 5 月 11 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutVisionConsoleReadOnlyAccess

描述：提供对 Amazon Lookout for Vision 的只读访问权限以及对所需服务和控制台依赖项的限定访问权限。

AmazonLookoutVisionConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutVisionConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 11 日 19:32 UTC
- 编辑时间：2021 年 12 月 9 日 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutVisionFullAccess

描述：提供对 Amazon Lookout for Vision 的完全访问权限以及对所需依赖项的限定访问权限。

AmazonLookoutVisionFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutVisionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 11 日 19:24 UTC
- 编辑时间：2021 年 5 月 11 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLookoutVisionReadOnlyAccess

描述：提供对 Amazon Lookout for Vision 的只读访问权限和对所需依赖项的限定访问权限。

AmazonLookoutVisionReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonLookoutVisionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 5 月 11 日 19:11 UTC
- 编辑时间：2021 年 12 月 9 日 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningBatchPredictionsAccess

描述：授予用户请求 Amazon Machine Learning 批量预测的权限。

AmazonMachineLearningBatchPredictionsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningBatchPredictionsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:12 UTC
- 编辑时间：2015 年 4 月 9 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
```

```
        "machinelearning:UpdateBatchPrediction"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningCreateOnlyAccess

描述：为非预测型 Amazon Machine Learning 资源提供创建权限。

AmazonMachineLearningCreateOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningCreateOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:18 UTC
- 编辑时间：2016 年 6 月 29 日，20:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningFullAccess

描述：提供对 Amazon Machine Learning 资源的完全访问权限。

AmazonMachineLearningFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningFullAccess 附加到您的用户、组和角色。

策略详细信息

- **类型：** AWS 托管策略

- 创建时间：2015 年 4 月 9 日 17:25 UTC
- 编辑时间：2015 年 4 月 9 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

描述：授予用户创建和删除 Amazon Machine Learning 模型的实时终端节点的权限。

AmazonMachineLearningManageRealTimeEndpointOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningManageRealTimeEndpointOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:32 UTC
- 编辑时间：2015 年 4 月 9 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonMachineLearningManageRealTimeEndpointOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningReadOnlyAccess

描述：提供对 Amazon Machine Learning 资源的只读访问权限。

AmazonMachineLearningReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:40 UTC
- 编辑时间：2015 年 4 月 9 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

描述：授予用户请求 Amazon Machine Learning 实时预测的权限。

AmazonMachineLearningRealTimePredictionOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningRealTimePredictionOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:44 UTC
- 编辑时间：2015 年 4 月 9 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonMachineLearningRealTimePredictionOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

描述：允许 Machine Learning 为 Redshift 数据源配置和使用你的 Redshift 集群和 S3 暂存位置。

AmazonMachineLearningRoleforRedshiftDataSourceV3是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonMachineLearningRoleforRedshiftDataSourceV3 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 24 日 18:00 UTC
- 编辑时间：2020 年 6 月 24 日 18:00 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMacieFullAccess

描述：提供对亚马逊 Macie 的完全访问权限。

AmazonMacieFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMacieFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 14:54 UTC
- 编辑时间：2022 年 7 月 1 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMacieHandshakeRole

描述：授予创建 Amazon Macie 服务相关角色的权限。

AmazonMacieHandshakeRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMacieHandshakeRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 6 月 28 日 15:46 UTC
- 编辑时间：2018 年 6 月 28 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "iam:AWSServiceName": "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMacieReadOnlyAccess

描述：提供对亚马逊 Macie 的只读访问权限。

AmazonMacieReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMacieReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 15 日 21:50 UTC
- 编辑时间：2023 年 6 月 15 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",

```

```
    "macie2:BatchGetCustomDataIdentifiers",
    "macie2:SearchResources"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMacieServiceRole

描述：授予 Macie 对您账户中资源依赖关系的只读访问权限，以便启用数据分析。

AmazonMacieServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMacieServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 14:53 UTC
- 编辑时间：2017 年 8 月 14 日 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMacieServiceRolePolicy

描述：亚马逊 Macie 的服务关联角色

AmazonMacieServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 19 日 22:17 UTC
- 编辑时间：2022 年 5 月 19 日 19:16 UTC

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

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonManagedBlockchainConsoleFullAccess

描述：提供通过 Amazon Managed Blockchain 的完全访问权限 AWS Management Console

AmazonManagedBlockchainConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonManagedBlockchainConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2019 年 4 月 29 日 21:23 UTC
- 编辑时间：2019 年 4 月 29 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonManagedBlockchainFullAccess

描述：提供对亚马逊托管区块链的完全访问权限。

AmazonManagedBlockchainFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonManagedBlockchainFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 29 日 21:39 UTC
- 编辑时间：2019 年 4 月 29 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonManagedBlockchainReadOnlyAccess

描述：提供对亚马逊托管区块链的只读访问权限。

AmazonManagedBlockchainReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonManagedBlockchainReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 30 日 18:17 UTC
- 编辑时间：2019 年 4 月 30 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "managedblockchain:Get*",
      "managedblockchain:List*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonManagedBlockchainServiceRolePolicy

描述：允许访问亚马逊托管区块链 AWS 服务 及其使用或管理的资源

AmazonManagedBlockchainServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 1 月 17 日 19:51 UTC
- 编辑时间：2020 年 1 月 17 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMCSFullAccess

描述：提供对亚马逊托管 Apache Cassandra 服务的完全访问权限

AmazonMCSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMCSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 13:45 UTC
- 编辑时间：2020 年 4 月 17 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMCSReadOnlyAccess

描述：提供对亚马逊托管 Apache Cassandra 服务的只读访问权限

AmazonMCSReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMCSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 13:46 UTC
- 编辑时间：2020 年 4 月 17 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMechanicalTurkFullAccess

描述：提供对 Amazon Mechanical Turk 中所有 API 的完全访问权限。

AmazonMechanicalTurkFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMechanicalTurkFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 11 日 19:08 UTC
- 编辑时间：2015 年 12 月 11 日 19:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMechanicalTurkReadOnly

描述：提供对 Amazon Mechanical Turk 中只读 API 的访问权限。

AmazonMechanicalTurkReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonMechanicalTurkReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 11 日 19:08 UTC

- 编辑时间：2019 年 9 月 25 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMemoryDBFullAccess

描述：通过提供对 Amazon MemoryDB 的完全访问权限。AWS Management Console

AmazonMemoryDBFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonMemoryDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 8 日 19:24 UTC
- 编辑时间：2021 年 10 月 8 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMemoryDBReadOnlyAccess

描述：通过提供对 Amazon MemoryDB 的只读访问权限。AWS Management Console

AmazonMemoryDBReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMemoryDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 8 日 19:27 UTC
- 编辑时间：2021 年 10 月 8 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMobileAnalyticsFinancialReportAccess

描述：提供对所有报告（包括所有应用程序资源的财务数据）的只读访问权限。

AmazonMobileAnalyticsFinancialReportAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMobileAnalyticsFinancialReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMobileAnalyticsFullAccess

描述：提供对所有应用程序资源的完全访问权限。

AmazonMobileAnalyticsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMobileAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMobileAnalyticsNon-financialReportAccess

描述：提供对所有应用程序资源的非财务报告的只读访问权限。

AmazonMobileAnalyticsNon-financialReportAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMobileAnalyticsNon-financialReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMobileAnalyticsWriteOnlyAccess

描述：为所有应用程序资源提供只写入权限来放置事件数据。（推荐用于 SDK 集成）

AmazonMobileAnalyticsWriteOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMobileAnalyticsWriteOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [  
  {  
    "Effect" : "Allow",  
    "Action" : "mobileanalytics:PutEvents",  
    "Resource" : "*"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMonitronFullAccess

描述：提供管理 Amazon Monitron 的完全访问权限

AmazonMonitronFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMonitronFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 2 日 22:40 UTC
- 编辑时间：2022 年 6 月 8 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMQApiFullAccess

描述：通过我们的 API/SDK 提供对亚马逊MQ的完全访问权限。

AmazonMQApiFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonMQApiFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 18 日 20:31 UTC
- 编辑时间：2020 年 11 月 4 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMQApiReadOnlyAccess

描述：通过我们的 API/SDK 提供对亚马逊MQ的只读访问权限。

AmazonMQApiReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonMQApiReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 18 日 20:31 UTC
- 编辑时间：2018 年 12 月 18 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
    },
  ],
}
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMQFullAccess

描述：通过提供对 AmazonMQ 的完全访问权限。AWS Management Console

AmazonMQFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 15:28 UTC
- 编辑时间：2020 年 11 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMQReadOnlyAccess

描述：通过提供对 AmazonMQ 的只读访问权限。AWS Management Console

AmazonMQReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMQReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 15:30 UTC
- 编辑时间：2017 年 11 月 28 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMQServiceRolePolicy

描述：AWS Amazon MQ 的服务关联角色政策

AmazonMQServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2020 年 11 月 4 日 16:07 UTC
- 编辑时间 : 2020 年 11 月 4 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMSKConnectReadOnlyAccess

描述：提供对亚马逊 MSK Connect 的只读访问权限

AmazonMSKConnectReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMSKConnectReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 20 日 10:18 UTC
- 编辑时间：2021 年 10 月 18 日 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMSKFullAccess

描述：提供对 Amazon MSK 的完全访问权限及其依赖项所需的其他权限。

AmazonMSKFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMSKFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 14 日 22:07 UTC
- 编辑时间：2023 年 10 月 18 日 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMSKReadOnlyAccess

描述：提供对 Amazon MSK 的只读访问权限

AmazonMSKReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonMSKReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2019 年 1 月 14 日 22:28 UTC
- 编辑时间：2019 年 1 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonMWAAServiceRolePolicy

描述：Amazon 托管工作流程在 Apache Airflow 中使用的服务关联角色。

AmazonMWAAServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 24 日 14:13 UTC
- 编辑时间：2022 年 11 月 17 日 00:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonNimbleStudio-LaunchProfileWorker

描述：此策略授予 Nimble Studio Launch Profile 工作人员访问所需资源的权限。将此策略附加到由 Nimble Studio Builder 创建的 EC2 实例。

AmazonNimbleStudio-LaunchProfileWorker 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonNimbleStudio-LaunchProfileWorker 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 28 日 04:47 UTC
- 编辑时间：2021 年 4 月 28 日 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonNimbleStudio-StudioAdmin

描述：本策略允许访问与工作室管理员关联的 Amazon Nimble Studio 资源以及其他服务中的相关工作室资源。将此策略附加到与您的 Studio 关联的管理员角色。

AmazonNimbleStudio-StudioAdmin 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonNimbleStudio-StudioAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 28 日 04:47 UTC
- 编辑时间：2023 年 9 月 22 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonNimbleStudio-StudioUser

描述：本策略允许访问与工作室用户关联的 Amazon Nimble Studio 资源以及其他服务中的相关工作室资源。将此策略附加到与您的 Studio 关联的用户角色。

AmazonNimbleStudio-StudioUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonNimbleStudio-StudioUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 28 日 04:48 UTC
- 编辑时间：2023 年 9 月 22 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOmicsFullAccess

描述：提供对 Amazon Omics 和其他必需 AWS 服务内容的完全访问权限。此策略允许用户查看和接受 RAM 共享邀请，以访问用户的 AWS 账户以外的资源。

AmazonOmicsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOmicsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 24 日 00:59 UTC
- 编辑时间：2023 年 2 月 24 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOmicsReadOnlyAccess

描述：提供对 Amazon Omics 的只读访问权限

AmazonOmicsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOmiccsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 29 日 04:17 UTC
- 编辑时间：2022 年 11 月 29 日 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmiccsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOneEnterpriseFullAccess

描述：此策略授予管理权限，允许访问所有 Amazon One Enterprise 资源和操作。

AmazonOneEnterpriseFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOneEnterpriseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 04:58
- 编辑时间：世界标准时间 2023 年 11 月 28 日 04:58
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOneEnterpriseInstallerAccess

描述：此策略授予有限的读取和写入权限，允许安装和激活设备。

AmazonOneEnterpriseInstallerAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOneEnterpriseInstallerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 05:00
- 编辑时间：世界标准时间 2023 年 11 月 28 日 05:00
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "InstallerAccessStatementID",
    "Effect" : "Allow",
    "Action" : [
      "one:CreateDeviceActivationQrCode",
      "one:GetDeviceInstance",
      "one:GetSite",
      "one:GetSiteAddress",
      "one:ListDeviceInstances",
      "one:ListSites"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOneEnterpriseReadOnlyAccess

描述：该政策授予对所有 Amazon One Enterprise 资源和操作的只读权限。

AmazonOneEnterpriseReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOneEnterpriseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 04:59

- 编辑时间：世界标准时间 2023 年 11 月 28 日 04:59
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchDashboardsServiceRolePolicy

描述：提供对 Amazon OpenSearch 控制面板服务的访问权限以访问其他 AWS 服务，例如 CloudWatch 代表您访问其他服务

AmazonOpenSearchDashboardsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 12 月 22 日 19:38
- 编辑时间：世界标准时间 2023 年 12 月 22 日 19:38
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

描述：允许 OpenSearch DirectQuery 服务访问 AWS Glue API，以便代表您创建资源。

AmazonOpenSearchDirectQueryGlueCreateAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchDirectQueryGlueCreateAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 5 月 6 日 12:24
- 编辑时间：世界标准时间 2024 年 5 月 6 日 12:24
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "glue:CreateDatabase",
    "glue:CreatePartition",
    "glue:CreateTable",
    "glue:BatchCreatePartition"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchIngestionFullAccess

描述：允许 Amazon OpenSearch Ingestion 代表您访问其他 AWS 服务。

AmazonOpenSearchIngestionFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchIngestionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 26 日 18:11 UTC
- 编辑时间：2023 年 4 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchIngestionReadOnlyAccess

描述：提供对 Amazon OpenSearch Ingestion 服务的只读访问权限

AmazonOpenSearchIngestionReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchIngestionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 26 日 18:09 UTC
- 编辑时间：2023 年 4 月 26 日 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "Effect" : "Allow",
    "Action" : [
      "osis:GetPipeline",
      "osis:GetPipelineChangeProgress",
      "osis:GetPipelineBlueprint",
      "osis:ListPipelineBlueprints",
      "osis:ListPipelines",
      "osis:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchIngestionServiceRolePolicy

描述：允许 Amazon OpenSearch Ingestion 服务代表您访问其他 AWS 服务。

AmazonOpenSearchIngestionServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 18 日 16:49 UTC
- 编辑时间：2022 年 11 月 18 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchServerlessServiceRolePolicy

描述：允许 Amazon OpenSearch Serverless 代表您访问其他 AWS 服务，例如 CloudWatch API。

AmazonOpenSearchServerlessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 24 日 19:50 UTC
- 编辑时间：2022 年 11 月 24 日 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/AOSS"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchServiceCognitoAccess

描述：提供对 Amazon Cognito 配置服务的访问权限。

AmazonOpenSearchServiceCognitoAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchServiceCognitoAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 2 日 06:31 UTC
- 编辑时间：2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchServiceFullAccess

描述：提供对 Amazon OpenSearch 服务配置服务的完全访问权限。

AmazonOpenSearchServiceFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 8 日 05:33 UTC
- 编辑时间：2021 年 9 月 8 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "es:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchServiceReadOnlyAccess

描述：提供对亚马逊 OpenSearch 服务配置服务的只读访问权限。

AmazonOpenSearchServiceReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonOpenSearchServiceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 8 日 05:38 UTC
- 编辑时间：2021 年 9 月 8 日 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonOpenSearchServiceRolePolicy

描述：允许亚马逊 OpenSearch 服务代表您访问其他 AWS 服务，例如 EC2 联网 API。

AmazonOpenSearchServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2021 年 8 月 26 日 09:27 UTC
- 编辑时间：2023 年 10 月 23 日 07:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
},
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPersonalizeFullAccess

描述：通过 AWS Management Console 和软件开发工具包提供对 Amazon Personalize 的完全访问权限。还提供对相关服务（例如 S3 CloudWatch）的选择访问权限。

AmazonPersonalizeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPersonalizeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 12 月 4 日 22:24 UTC
- 编辑时间：2019 年 5 月 30 日 23:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPollyFullAccess

描述：授予对 Amazon Polly 服务和资源的完全访问权限。

AmazonPollyFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPollyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 18:59 UTC
- 编辑时间：2016 年 11 月 30 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPollyReadOnlyAccess

描述：授予对 Amazon Polly 资源的只读访问权限。

AmazonPollyReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPollyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 18:59 UTC
- 编辑时间：2018 年 7 月 17 日 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPrometheusConsoleFullAccess

描述：授予控制台中 AWS 托管 Prometheus 资源的完全访问权限 AWS

AmazonPrometheusConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPrometheusConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:11 UTC
- 编辑时间：2022 年 10 月 24 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPrometheusFullAccess

描述：授予对 AWS 托管 Prometheus 资源的完全访问权限

AmazonPrometheusFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPrometheusFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:10 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 20:16
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPrometheusQueryAccess

描述：授予对 AWS 托管 Prometheus 资源运行查询的权限

AmazonPrometheusQueryAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPrometheusQueryAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 19 日 01:02 UTC
- 编辑时间：2020 年 12 月 19 日 01:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "aps:GetLabels",
      "aps:GetMetricMetadata",
      "aps:GetSeries",
      "aps:QueryMetrics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPrometheusRemoteWriteAccess

描述：授予对 AWS 托管 Prometheus 工作空间的只写访问权限

AmazonPrometheusRemoteWriteAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonPrometheusRemoteWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 19 日 01:04 UTC
- 编辑时间：2020 年 12 月 19 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonPrometheusScrapperServiceRolePolicy

描述：为 Prometheus Collector 提供对亚马逊托管服务管理或使用的 AWS 资源的访问权限

AmazonPrometheusScrapperServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 14:19
- 编辑时间：世界标准时间 2024 年 4 月 26 日 20:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "AMPAgentlessScrapper"
    ]
  }
},
{
  "Sid" : "TagManagement",
"Effect" : "Allow",
"Action" : "ec2:CreateTags",
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : "CreateNetworkInterface"
  },
  "Null" : {
    "aws:RequestTag/AMPAgentlessScrapper" : "false"
  }
},
{
  "Sid" : "ENIUpdating",
"Effect" : "Allow",
"Action" : [
  "ec2>DeleteNetworkInterface",
  "ec2:ModifyNetworkInterfaceAttribute"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "ec2:ResourceTag/AMPAgentlessScrapper" : "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}"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonQFullAccess

描述：提供完全访问权限以实现与 Amazon Q 的互动

AmazonQFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 16:00
- 编辑时间：世界标准时间 2024 年 4 月 29 日 17:02
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonQLDBConsoleFullAccess

描述：通过提供对 Amazon QLDB 的完全访问权限。AWS Management Console

AmazonQLDBConsoleFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonQLDBConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 9 月 5 日 18:24 UTC
- 编辑时间：2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonQLDBFullAccess

描述：通过服务 API 提供对 Amazon QLDB 的完全访问权限。

AmazonQLDBFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonQLDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 9 月 5 日 18:23 UTC
- 编辑时间：2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonQLDBReadOnly

描述：提供对亚马逊 QLDB 的只读访问权限。

AmazonQLDBReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonQLDBReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 9 月 5 日 18:19 UTC
- 编辑时间：2021 年 7 月 2 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSBetaServiceRolePolicy

描述：允许 Amazon RDS 代表您管理 AWS 资源。

AmazonRDSBetaServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 2 日 19:41 UTC
- 编辑时间：2022 年 12 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "sns:Publish"
    ],
    "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"
      }
    }
  }
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSCustomInstanceProfileRolePolicy

描述：允许 Amazon RDS Custom 通过 EC2 实例配置文件执行各种自动化操作和数据库管理任务。

AmazonRDSCustomInstanceProfileRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSCustomInstanceProfileRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 2 月 27 日 17:42
- 编辑时间：世界标准时间 2024 年 2 月 27 日 17:42
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
```

```
    ],
    "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" : "cwUploadPermission",
    "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-*"
    },
    "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSCustomPreviewServiceRolePolicy

描述：Amazon RDS 自定义预览版服务角色策略

AmazonRDSCustomPreviewServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 8 日 21:44 UTC
- 编辑时间：2023 年 9 月 20 日 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "RequireImsdV2",
    "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-*"
    ],
    "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-*"
    ],
    "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-*",
  "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"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
```

```
        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "servicequota1",
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSCustomServiceRolePolicy

描述：允许 Amazon RDS Custom 代表您管理 AWS 资源。

AmazonRDSCustomServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型：**服务相关角色策略
- **创建时间：**2021 年 10 月 8 日 21:39 UTC
- **编辑时间：**世界标准时间 2024 年 4 月 19 日 15:15
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy

策略版本

策略版本 : v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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-*"
```

```
    ],
    "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-*"
    ],
    "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"
    ]
  }
},
{
  "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" : "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-*",
  "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"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "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"
      ]
    }
  }
},
{
  "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"
        ]
    }
},
{
    "Sid" : "servicequota1",
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSDDataFullAccess

描述：允许使用 RDS 数据 API、用于 RDS 数据库凭证的密钥存储 API 以及数据库控制台查询管理 API 在中的 Aurora Serverless 集群上执行 SQL 语句的完全访问权限。AWS 账户

AmazonRDSDDataFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSDDataFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 20 日 21:29 UTC
- 编辑时间：2019 年 11 月 20 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSDDataFullAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSDirectoryServiceAccess

描述：允许 RDS 代表客户访问已加入域的 SQL Server 数据库实例的 Directory Service Managed AD。

AmazonRDSDirectoryServiceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSDirectoryServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 26 日 02:02 UTC
- 编辑时间：2019 年 5 月 15 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSEnhancedMonitoringRole

描述：提供对 Cloudwatch 的访问权限以实现 RDS 增强监控

AmazonRDSEnhancedMonitoringRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSEnhancedMonitoringRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 11 日 19:58 UTC
- 编辑时间：2015 年 11 月 11 日 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSFullAccess

描述：通过提供对 Amazon RDS 的完全访问权限 AWS Management Console。

AmazonRDSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 8 月 17 日 23:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSPerformanceInsightsFullAccess

描述：提供通过 RDS Performance Insights 的完整访问权限 AWS Management Console

AmazonRDSPerformanceInsightsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSPerformanceInsightsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 15 日 23:41 UTC
- 编辑时间：2023 年 10 月 23 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AmazonRDSPerformanceInsightsAnalysisReportFullAccess",
    "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" : "*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSPerformanceInsightsReadOnly

描述：RDS 性能 Insights 的只读策略

AmazonRDSPerformanceInsightsReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSPerformanceInsightsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 5 日 00:02 UTC
- 编辑时间：2023 年 10 月 23 日 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSPreviewServiceRolePolicy

描述：Amazon RDS 预览版服务角色策略

AmazonRDSPreviewServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 31 日 18:02 UTC
- 编辑时间：2023 年 10 月 4 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "sns:Publish"
    ],
    "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"
  }
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSReadOnlyAccess

描述：通过提供对 Amazon RDS 的只读访问权限 AWS Management Console。

AmazonRDSReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRDSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 4 月 14 日 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSServiceRolePolicy

描述：允许 Amazon RDS 代表您管理 AWS 资源。

AmazonRDSServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 1 月 8 日 18:17 UTC
- 编辑时间：世界标准时间 2024 年 1 月 19 日 15:10
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "Sns",
    "Effect" : "Allow",
```

```
"Action" : [
  "sns:Publish"
],
"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"
      }
    }
  }
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftAllCommandsFullAccess

描述：此策略包括运行 SQL 命令以复制、加载、卸载、查询和分析 Amazon Redshift 上的数据的权限。该策略还授予为相关服务（例如 Amazon S3、Amazon CloudWatch 日志、Amazon 或 AWS Glue）运行精选语句的权限。 SageMaker

AmazonRedshiftAllCommandsFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftAllCommandsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 4 日 00:48 UTC
- 编辑时间：2021 年 11 月 25 日 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftDataFullAccess

描述：本策略提供对亚马逊 Redshift 数据 API 的完全访问权限。此策略还授予访问其他所需服务的限定访问权限。

AmazonRedshiftDataFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftDataFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 9 日 19:23 UTC
- 编辑时间：2023 年 4 月 7 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftFullAccess

描述：通过提供对亚马逊 Redshift 的完全访问权限。AWS Management Console

AmazonRedshiftFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2022 年 7 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditor

描述：提供对 Amazon Redshift 查询编辑器和通过保存的查询的完全访问权限。AWS Management Console

AmazonRedshiftQueryEditor 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftQueryEditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 4 日 22:50 UTC
- 编辑时间：2021 年 2 月 16 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2FullAccess

描述：授予对 Amazon Redshift 查询编辑器 V2 操作和资源的完全访问权限。此策略还授予访问其他所需服务的访问权限。这包括列出 Amazon Redshift 集群、读取 KMS 中的密钥和别名以及在 AWS Secrets Manager 中管理查询编辑器 V2 密钥的权限。AWS

AmazonRedshiftQueryEditorV2FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:06 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:20
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2NoSharing

描述：允许在不共享资源的情况下使用 Amazon Redshift 查询编辑器 V2。被授予权限的主体只能读取、更新和删除自己的资源，但不能共享这些资源。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

AmazonRedshiftQueryEditorV2NoSharing 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2NoSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:18 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:25
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2ReadSharing

描述：允许在有限的资源共享下使用 Amazon Redshift 查询编辑器 V2。获得授权的主体可读取、写入和共享自己的资源。获得授权的主体可读取其与团队共享的资源，但不能更新。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

AmazonRedshiftQueryEditorV2ReadSharing 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2ReadSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:22 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:27
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
        }
    }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

描述：允许使用 Amazon Redshift 查询编辑器 V2 进行资源共享。获得授权的主体可读取、写入和共享自己的资源。授予主体可以读取和更新与其团队共享的资源。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

AmazonRedshiftQueryEditorV2ReadWriteSharing 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2ReadWriteSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:25 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:30
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:user}"
    }
  }
},
{
  "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}"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftReadOnlyAccess

描述：通过提供对亚马逊 Redshift 的只读访问权限。AWS Management Console

AmazonRedshiftReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRedshiftReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：世界标准时间 2024 年 2 月 8 日 00:24
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftServiceLinkedRolePolicy

描述：允许 Amazon Redshift 代表你呼叫 AWS 服务

AmazonRedshiftServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 18 日 19:19 UTC
- 编辑时间：世界标准时间 2024 年 3 月 15 日 20:00
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRekognitionCustomLabelsFullAccess

描述：此策略指定了 Amazon Rekognition 自定义标签功能所需的识别和 s3 权限。

AmazonRekognitionCustomLabelsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRekognitionCustomLabelsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 8 日 19:18 UTC
- 编辑时间：2022 年 8 月 16 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRekognitionFullAccess

描述：访问所有亚马逊 Rekognition API

AmazonRekognitionFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRekognitionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 14:40 UTC
- 编辑时间：2016 年 11 月 30 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRekognitionReadOnlyAccess

描述：访问所有 Read Read Rekognition API

AmazonRekognitionReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRekognitionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2016 年 11 月 30 日 14:58 UTC
- 编辑时间 : 2023 年 11 月 8 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

策略版本

策略版本 : v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRekognitionServiceRole

描述：允许 Rekognition 代表你呼叫服务。AWS

AmazonRekognitionServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRekognitionServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间 : 2017 年 11 月 29 日 16:52 UTC
- 编辑时间 : 2017 年 11 月 29 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53AutoNamingFullAccess

描述：提供对所有 Route 53 自动命名操作的完全访问权限。

AmazonRoute53AutoNamingFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53AutoNamingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 1 月 18 日 18:40 UTC
- 编辑时间：2018 年 1 月 18 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53AutoNamingReadOnlyAccess

描述：提供对所有 Route 53 自动命名操作的只读访问权限。

AmazonRoute53AutoNamingReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53AutoNamingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 1 月 18 日 03:02 UTC
- 编辑时间：2018 年 1 月 18 日 03:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53AutoNamingRegistrantAccess

描述：提供对 Route 53 自动命名操作的注册人级别访问权限。

AmazonRoute53AutoNamingRegistrantAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53AutoNamingRegistrantAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 12 日 22:33 UTC
- 编辑时间：2018 年 3 月 12 日 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53DomainsFullAccess

描述：提供对所有 Route53 Domains 操作和“创建托管区域”的完全访问权限，以允许将托管区域作为域注册的一部分创建。

AmazonRoute53DomainsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53DomainsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53DomainsReadOnlyAccess

描述：提供对 Route53 域列表和操作的访问权限。

AmazonRoute53DomainsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53DomainsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53FullAccess

描述：通过提供对所有 Amazon Route 53 的完全访问权限 AWS Management Console。

AmazonRoute53FullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 12 月 20 日 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",

```



```
    "cloudfront:ListDistributions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticbeanstalk:DescribeEnvironments",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRegions",
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : "arn:aws:apigateway:*::/domainnames"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53ProfilesFullAccess

描述：此政策授予对 Amazon Route 53 个人资料资源的完全访问权限。

AmazonRoute53ProfilesFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53ProfilesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 30 日 18:30
- 编辑时间：世界标准时间 2024 年 4 月 30 日 18:30
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
      ]
    }
  ]
}
```

```
    "route53resolver:GetFirewallRuleGroup",
    "route53resolver:GetResolverConfig",
    "route53resolver:GetResolverDnssecConfig",
    "route53resolver:GetResolverQueryLogConfig",
    "route53resolver:GetResolverRule",
    "ec2:DescribeVpcs",
    "route53:GetHostedZone"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53ProfilesReadOnlyAccess

描述：此政策授予对 Amazon Route 53 个人资料资源的只读访问权限。

AmazonRoute53ProfilesReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53ProfilesReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 30 日 18:29
- 编辑时间：世界标准时间 2024 年 4 月 30 日 18:29
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53ReadOnlyAccess

描述：通过提供对所有 Amazon Route 53 的只读访问权限 AWS Management Console。

AmazonRoute53ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2016 年 11 月 15 日 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryClusterFullAccess

描述：提供对 Amazon Route 53 恢复集群的完全访问权限

AmazonRoute53RecoveryClusterFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53RecoveryClusterFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:37 UTC
- 编辑时间：2021 年 8 月 18 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "route53-recovery-cluster:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

描述：提供对 Amazon Route 53 恢复集群的只读访问权限

AmazonRoute53RecoveryClusterReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53RecoveryClusterReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 17:36 UTC
- 编辑时间：2022 年 4 月 1 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryControlConfigFullAccess

描述：提供对 Amazon Route 53 恢复控制 Config 的完全访问权限

AmazonRoute53RecoveryControlConfigFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53RecoveryControlConfigFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 8 月 18 日 17:48 UTC
- 编辑时间：2021 年 8 月 18 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

描述：提供对 Amazon Route 53 恢复控制 Config 的只读访问权限

AmazonRoute53RecoveryControlConfigReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AmazonRoute53RecoveryControlConfigReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:01 UTC
- 编辑时间：2023 年 10 月 18 日 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"   
}   
]   
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryReadinessFullAccess

描述：提供对 Amazon Route 53 恢复准备的完全访问权限

AmazonRoute53RecoveryReadinessFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53RecoveryReadinessFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 16:45 UTC
- 编辑时间：2021 年 8 月 18 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

描述：提供对 Amazon Route 53 恢复就绪状态的只读访问权限

AmazonRoute53RecoveryReadinessReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53RecoveryReadinessReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:11 UTC
- 编辑时间：2021 年 11 月 9 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53ResolverFullAccess

描述：Route 53 Resolver 的完全访问策略

AmazonRoute53ResolverFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53ResolverFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 30 日 18:10 UTC
- 编辑时间：2020 年 7 月 17 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Effect" : "Allow",
"Action" : [
  "route53resolver:*",
  "ec2:DescribeSubnets",
  "ec2:CreateNetworkInterface",
  "ec2>DeleteNetworkInterface",
  "ec2:ModifyNetworkInterfaceAttribute",
  "ec2:DescribeNetworkInterfaces",
  "ec2:CreateNetworkInterfacePermission",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeVpcs",
  "ec2:DescribeAvailabilityZones"
],
"Resource" : [
  "*"
]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRoute53ResolverReadOnlyAccess

描述：Route 53 Resolver 的只读策略

AmazonRoute53ResolverReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonRoute53ResolverReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2019 年 5 月 30 日 18:11 UTC
- 编辑时间 : 2019 年 9 月 27 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonS3FullAccess

描述：通过提供对所有存储桶的完全访问权限。 AWS Management Console

AmazonS3FullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonS3FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2021 年 9 月 27 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonS3ObjectLambdaExecutionRolePolicy

描述：提供 AWS Lambda 函数与亚马逊 S3 对象 Lambda 交互的权限。还授予 Lambda 写入日志的权限。CloudWatch

AmazonS3ObjectLambdaExecutionRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonS3ObjectLambdaExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 8 月 18 日 10:07 UTC
- 编辑时间：2021 年 8 月 18 日 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "s3-object-lambda:WriteGetObjectResponse"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonS3OutpostsFullAccess

描述：通过 Outposts 提供对 Amazon S3 的完全访问权限。AWS Management Console

AmazonS3OutpostsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonS3OutpostsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 2 日 17:26 UTC
- 编辑时间：2020 年 10 月 2 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonS3OutpostsReadOnlyAccess

描述：通过 Outposts 提供对 Amazon S3 的只读访问权限。AWS Management Console

AmazonS3OutpostsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonS3OutpostsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 2 日 18:55 UTC
- 编辑时间：2020 年 10 月 2 日 18:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonS3ReadOnlyAccess

描述：通过提供对所有存储桶的只读访问权限。AWS Management Console

AmazonS3ReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonS3ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 8 月 10 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : [
      "s3:Get*",
      "s3:List*",
      "s3:Describe*",
      "s3-object-lambda:Get*",
      "s3-object-lambda:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

描述：AWS 服务目录服务使用的服务角色策略，用于配置亚马逊产品 SageMaker 组合中的商品。向一组相关服务授予权限 CodePipeline，包括、CodeBuild、CodeCommit CloudFormation、Glue 等。

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 27 日 18:48 UTC
- 编辑时间：世界标准时间 2024 年 6 月 12 日 18:06

- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:PATCH"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/account"
  ]
},
{
  "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*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "cloudformation:ValidateTemplate"
  ],
  "Resource" : "*"
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:UpdateProject"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codecommit:CreateCommit",
    "codecommit>CreateRepository",
    "codecommit>DeleteRepository",
    "codecommit:GetRepository",
    "codecommit:TagResource"
  ],
  "Resource" : [
    "arn:aws:codecommit:*:*:codecommit-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codecommit:ListRepositories"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "codepipeline:CreatePipeline",
    "codepipeline>DeletePipeline",
    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineState",
    "codepipeline:StartPipelineExecution",
    "codepipeline:TagResource",
    "codepipeline:UpdatePipeline"
  ],
  "Resource" : [
    "arn:aws:codepipeline:*:*:codepipeline-*"
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cognito-idp:CreateUserPool",
    "cognito-idp:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "sagemaker:launch-source"
      ]
    }
  }
},
{
  "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" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr>DeleteRepository",
```

```
    "ecr:TagResource"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events>DeleteRule",
    "events:DisableRule",
    "events:EnableRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "firehose>CreateDeliveryStream",
    "firehose>DeleteDeliveryStream",
    "firehose:DescribeDeliveryStream",
    "firehose:StartDeliveryStreamEncryption",
    "firehose:StopDeliveryStreamEncryption",
    "firehose:UpdateDestination"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
},
{
  "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-*"
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateClassifier",
    "glue>DeleteClassifier",
    "glue>DeleteCrawler",
    "glue>DeleteJob",
    "glue>DeleteTrigger",
    "glue>DeleteWorkflow",
    "glue:StopCrawler"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateWorkflow"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:workflow/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateJob"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:job/sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateCrawler",
    "glue:GetCrawler"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:crawler/sagemaker-*"
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```

        "sagemaker:*"
    ]
}
},
{
    "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:*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : [
        "arn:aws:s3:::sagemaker-*"
    ]
},
{
    "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-*"
},
{
  "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:*:*:*"
  ]
},
{
  "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:*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateImage",
    "sagemaker>DeleteImage",
    "sagemaker:DescribeImage",
    "sagemaker:UpdateImage",
    "sagemaker>ListTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:image/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states:CreateStateMachine",
    "states>DeleteStateMachine",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
  "Condition" : {
    "StringEquals" : {

```

```
        "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
    }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasAIServicesAccess

描述：为 Amazon SageMaker Canvas 提供使用人工智能服务的权限，以支持即用型人工智能解决方案。随着 Amazon SageMaker Canvas 增加支持，该政策将为服务添加更多变更权限。

AmazonSageMakerCanvasAIServicesAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasAIServicesAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 23 日 22:36 UTC
- 编辑时间：世界标准时间 2023 年 11 月 29 日 14:47
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textextract",
      "Effect" : "Allow",
      "Action" : [
        "textextract:AnalyzeDocument",
        "textextract:AnalyzeExpense",
        "textextract:AnalyzeID",
        "textextract:StartDocumentAnalysis",
        "textextract:StartExpenseAnalysis",
        "textextract:GetDocumentAnalysis",
        "textextract: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"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasBedrockAccess

描述：此策略通过提供对 S3 等下游服务的访问权限，授予在 C SageMaker anvas 中使用 Amazon Bedrock 的权限。

AmazonSageMakerCanvasBedrockAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasBedrockAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 2 月 2 日 18:37
- 编辑时间：世界标准时间 2024 年 2 月 2 日 18:37
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasDataPrepFullAccess

描述：提供对 Amazon SageMaker 资源和操作的完全访问权限，以便在 Canvas 中准备数据。该策略还提供对相关服务（例如 S3、IAM、KMS、RDS、Lambda、CloudWatch、RDS、RDS、Redshift、Athena、Glue、Secrets Manager）的精选访问权限。EventBridge 此政策应附加到 Amazon SageMaker 域名/用户配置文件执行角色。

AmazonSageMakerCanvasDataPrepFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasDataPrepFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 10 月 27 日 22:56 UTC
- 编辑时间：世界标准时间 2023 年 12 月 8 日 02:53
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasDirectDeployAccess

描述：允许 Amazon SageMaker Canvas 创建、管理和查看通过 Canvas 创建的终端节点的终端节点详细信息。允许 Amazon SageMaker Canvas 从中 CloudWatch 检索终端节点调用指标。

AmazonSageMakerCanvasDirectDeployAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasDirectDeployAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间 : 2023 年 10 月 6 日 18:11 UTC
- 编辑时间 : 2023 年 10 月 6 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasForecastAccess

描述：此政策授予在 Amazon Forecast 中使用 SageMaker Canvas 通常所需的权限。

AmazonSageMakerCanvasForecastAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasForecastAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 8 月 24 日 20:04 UTC
- 编辑时间：2022 年 8 月 24 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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-*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCanvasFullAccess

描述：提供对 Amazon SageMaker Canvas 资源和操作的完全访问权限。该策略还提供对相关服务（例如 S3、IAM、VPC、ECR、CloudWatch logs、Redshift、Secrets Manager 和 Forecast）的精选访问权限。此策略应附加到 Amazon SageMaker 域名/用户配置文件执行角色。

AmazonSageMakerCanvasFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerCanvasFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 9 日 00:44 UTC
- 编辑时间：世界标准时间 2024 年 1 月 24 日 22:01
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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>DeleteEndpoint",
    "sagemaker:DescribeCompilationJob",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeProcessingJob",
    "sagemaker:DescribeAutoMLJob",
    "sagemaker:DescribeAutoMLJobV2",
    "sagemaker:ListCandidatesForAutoMLJob",
    "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" : "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"
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerClusterInstanceRolePolicy

描述：此策略授予使用 Amazon SageMaker 集群通常所需的权限。

AmazonSageMakerClusterInstanceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerClusterInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 15:11
- 编辑时间：世界标准时间 2023 年 11 月 29 日 15:11
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerCoreServiceRolePolicy

描述：Amazon SageMaker 核心服务的服务关联角色托管策略

AmazonSageMakerCoreServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型**：服务相关角色策略
- **创建时间**：2020 年 12 月 21 日 21:40 UTC
- **编辑时间**：2020 年 12 月 21 日 21:40 UTC
- **ARN**: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerEdgeDeviceFleetPolicy

描述：提供 SageMaker Edge 使用默认云连接为客户创建和管理设备队列所需的权限。

AmazonSageMakerEdgeDeviceFleetPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerEdgeDeviceFleetPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 8 日 16:17 UTC
- 编辑时间：2020 年 12 月 8 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
}
```

```
    ]
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerFeatureStoreAccess

描述：提供为亚马逊 SageMaker FeatureStore 功能组启用离线商店所需的权限。

AmazonSageMakerFeatureStoreAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerFeatureStoreAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:24 UTC
- 编辑时间：2022 年 12 月 5 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerFullAccess

描述：SageMaker 通过 AWS Management Console 和 SDK 提供对 Amazon 的完全访问权限。还提供对相关服务（例如 S3、ECR、CloudWatch 日志）的精选访问权限。

AmazonSageMakerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 13:07 UTC
- 编辑时间：世界标准时间 2024 年 3 月 29 日 17:35
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

策略版本

策略版本：v26（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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" : "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerGeospatialExecutionRole

描述：此策略提供对使用 SageMaker 地理空间通常需要的服务的访问权限。

AmazonSageMakerGeospatialExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerGeospatialExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 11 月 30 日 10:08 UTC
- 编辑时间：2023 年 5 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerGeospatialFullAccess

描述：此政策授予的权限允许通过 AWS Management Console 和软件开发工具包对 Amazon SageMaker Geospatial 进行完全访问。

AmazonSageMakerGeospatialFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerGeospatialFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 11 月 30 日 10:06 UTC

- 编辑时间：2022 年 11 月 30 日 10:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerGroundTruthExecution

描述：提供对运行 SageMaker GroundTruth 标签作业所需的 AWS 服务的访问权限

AmazonSageMakerGroundTruthExecution 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerGroundTruthExecution 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 9 日 19:30 UTC
- 编辑时间：2022 年 4 月 29 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
        ]
      }
    }
  }
}
```

```
    ]
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerMechanicalTurkAccess

描述：提供针对任何 Workteam 创建 Amazon Agumentead AI FlowDefinition 资源的权限。

AmazonSageMakerMechanicalTurkAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerMechanicalTurkAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:19 UTC
- 编辑时间：2019 年 12 月 3 日 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerModelGovernanceUseAccess

描述：此 AWS 托管策略授予使用所有 Amazon SageMaker Governance 功能所需的权限。该策略还提供对相关服务（例如 S3、KMS）的部分访问权限。

AmazonSageMakerModelGovernanceUseAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerModelGovernanceUseAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 30 日 08:58 UTC
- 编辑时间：世界标准时间 2024 年 6 月 4 日 21:48

- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```



```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerModelRegistryFullAccess

描述：这是 Sagemaker 中模型注册表的新托管策略。此策略是一项独立的策略，可以附加到用户角色以访问 Sagemaker 中与模型注册表相关的功能。

AmazonSageMakerModelRegistryFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerModelRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 13 日 05:20 UTC
- 编辑时间：世界标准时间 2024 年 6 月 6 日 18:48
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerNotebooksServiceRolePolicy

描述：Amazon SageMaker 笔记本服务关联角色的托管策略

AmazonSageMakerNotebooksServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 18 日 20:27 UTC
- 编辑时间：世界标准时间 2024 年 5 月 22 日 19:18
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

描述：AWS ApiGateway 在亚马逊 SageMaker 产品组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 Lambda 和其他服务在内的相关服务集合授予权限。

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 1 日 15:06 UTC
- 编辑时间：2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

描述：Amazon 产品 SageMaker 组合 AWS CloudFormation 中 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 Lambda、APIGateway 和其他服务在内的相关服务子集授予权限。

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 1 日 15:06 UTC
- 编辑时间：2023 年 8 月 1 日 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

描述：AWS Lambda 在亚马逊 SageMaker 产品组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 Secrets Manager 和其他服务在内的相关服务集合授予权限。

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2023 年 8 月 1 日 15:05 UTC
- 编辑时间：2023 年 8 月 1 日 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerPipelinesIntegrations

描述：本 Amazon 托管策略授予在 SageMaker 模型构建管道中使用回调步骤和 Lambda 步骤通常所需的权限。它已添加 ExecutionRole 到 AmazonSageMaker-中，可以在设置 SageMaker Studio 时创建。也可以附加到任何其他用于创作或执行管道的角色。

AmazonSageMakerPipelinesIntegrations 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerPipelinesIntegrations 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 7 月 30 日 16:35 UTC
- 编辑时间：2023 年 2 月 17 日 21:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerReadOnly

描述：SageMaker 通过 AWS Management Console 和软件开发工具包提供对 Amazon 的只读访问权限。

AmazonSageMakerReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 13:07 UTC
- 编辑时间：2021 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

描述：AWS ApiGateWay 在亚马逊 SageMaker 产品组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 CloudWatch 日志和其他服务在内的一组相关服务授予权限。

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 3 月 25 日 04:25 UTC
- 编辑时间：2022 年 3 月 25 日 04:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

描述：Amazon 产品 SageMaker 组合 AWS CloudFormation 中 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向相关服务的子集（包括 SageMaker 和其他服务）授予权限。

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 3 月 25 日 04:26 UTC
- 编辑时间：2022 年 3 月 25 日 04:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ]
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

描述：Amazon 产品 SageMaker 组合 AWS CodeBuild 中 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向一部分相关服务（包括 CodePipeline CodeBuild 和其他）授予权限。

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 3 月 25 日 04:27 UTC
- 编辑时间：世界标准时间 2024 年 6 月 11 日 18:45
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AmazonSageMakerCodeBuildPassRolePermission",

```

```

    "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

描述：Amazon 产品 SageMaker 组合 AWS CodePipeline 中 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向一部分相关服务（包括 CodePipeline CodeBuild 和其他）授予权限。

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:53 UTC
- 编辑时间：世界标准时间 2024 年 6 月 11 日 18:37
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
    }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

描述：AWS CloudWatch 活动在亚马逊产品 SageMaker 组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向相关服务的子集（包括 CodePipeline 和其他服务）授予权限。

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:53 UTC
- 编辑时间：2022 年 2 月 22 日 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

描述：AWS Firehose 在亚马逊 SageMaker 产品组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 Firehose 和其他服务在内的相关服务集合授予权限。

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:54 UTC
- 编辑时间：2022 年 2 月 22 日 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "Effect" : "Allow",
    "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

描述：AWS Glue 在亚马逊产品 SageMaker 组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 Glue、S3 和其他服务在内的相关服务集合授予权限。

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:51 UTC
- 编辑时间：2022 年 8 月 26 日 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

描述：AWS Lambda 在亚马逊 SageMaker 产品组合中的 AWS ServiceCatalog 预配置产品中使用的服务角色策略。向包括 ECR、S3 和其他服务在内的相关服务集合授予权限。

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 4 日 16:34 UTC
- 编辑时间：世界标准时间 2024 年 6 月 11 日 18:57

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

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSecurityLakeAdministrator

描述：提供对 Amazon Security Lake 以及管理安全湖所需的相关服务的完全访问权限。

AmazonSecurityLakeAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSecurityLakeAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 30 日 22:04 UTC
- 编辑时间：世界标准时间 2024 年 2 月 23 日 16:01
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AllowRolePolicyActionsforSubscribersandSources",
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSecurityLakeMetastoreManager

描述：亚马逊 SecurityLake 元存储管理器 lambda 的政策，该政策允许访问 cloudwatch、S3、Glue 和 SQS。

AmazonSecurityLakeMetastoreManager 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSecurityLakeMetastoreManager 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 23 日 15:26
- 编辑时间：世界标准时间 2024 年 4 月 1 日 20:04
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSecurityLakePermissionsBoundary

描述：Amazon Security Lake 为第三方自定义源创建 IAM 角色以向数据湖写入数据，并供第三方订阅者使用来自数据湖的数据，并在创建这些角色时使用此策略来定义其权限边界。

AmazonSecurityLakePermissionsBoundary 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSecurityLakePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 29 日 14:11 UTC
- 编辑时间：世界标准时间 2024 年 5 月 14 日 20:39
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
        ]
    }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSESEFullAccess

描述：通过提供对 Amazon SES 的完全访问权限 AWS Management Console。

AmazonSESEFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSESEFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESEFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSESReadOnlyAccess

描述：通过提供对 Amazon SES 的只读访问权限 AWS Management Console。

AmazonSESReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSESReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 5 月 14 日 12:03
- ARN: arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSESServiceRolePolicy

描述：允许 SES 代表您的 SES 资源发布 Amazon CloudWatch 基本监控指标

AmazonSESServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 5 月 21 日 16:02
- 编辑时间：世界标准时间 2024 年 5 月 21 日 16:02
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
}
}
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSNSFullAccess

描述：通过提供对 Amazon SNS 的完全访问权限。AWS Management Console

AmazonSNSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSNSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSNSReadOnlyAccess

描述：通过提供对 Amazon SNS 的只读访问权限。AWS Management Console

AmazonSNSReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonSNSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSNSRole

描述：Amazon SNS 服务角色的默认策略。

AmazonSNSRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSNSRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSQSFullAccess

描述：通过提供对 Amazon SQS 的完全访问权限。AWS Management Console

AmazonSQSFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonSQSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSQSReadOnlyAccess

描述：通过提供对 Amazon SQS 的只读访问权限。AWS Management Console

AmazonSQSReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSQSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 5 月 24 日 18:16
- ARN: arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Sid" : "AmazonSQSReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl",
      "sqs:ListDeadLetterSourceQueues",
      "sqs:ListQueues",
      "sqs:ListMessageMoveTasks",
      "sqs:ListQueueTags"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMAutomationApproverAccess

描述：提供查看自动化执行和向等待批准的自动化发送批准决策的权限

AmazonSSMAutomationApproverAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMAutomationApproverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 7 日 23:07 UTC
- 编辑时间：2017 年 8 月 7 日 23:07 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMAutomationRole

描述 : 为 EC2 自动化服务提供执行自动化文档中定义的活动的权限

AmazonSSMAutomationRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMAutomationRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 5 日 22:09 UTC
- 编辑时间：2017 年 7 月 24 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMDirectoryServiceAccess

描述：此策略允许 SSM 代理代表客户访问 Directory Service 以加入托管实例的域名。

AmazonSSMDirectoryServiceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMDirectoryServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 3 月 15 日 17:44 UTC
- 编辑时间：2019 年 3 月 15 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "ds:DescribeDirectories"  
  ],  
  "Resource" : "*"   
}   
]   
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMFullAccess

描述：提供对 Amazon SSM 的完全访问权限。

AmazonSSMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 29 日 17:39 UTC
- 编辑时间：2019 年 11 月 20 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMMaintenanceWindowRole

描述：用于 EC2 维护窗口的服务角色

AmazonSSMMaintenanceWindowRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMMaintenanceWindowRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 1 日 15:57 UTC
- 编辑时间：2019 年 7 月 27 日 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",

```

```
    "resource-groups:ListGroupResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMManagedEC2InstanceDefaultPolicy

描述：此策略在 EC2 实例上启用 S AWS systems Manager 功能。

AmazonSSMManagedEC2InstanceDefaultPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMManagedEC2InstanceDefaultPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 30 日 20:54 UTC

- 编辑时间：2022 年 8 月 30 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSManagedEC2InstanceDefaultPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMManagedInstanceCore

描述：Amazon EC2 角色启用 S AWS systems Manager 服务核心功能的策略。

AmazonSSMManagedInstanceCore是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMManagedInstanceCore 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 3 月 15 日 17:22 UTC
- 编辑时间：2019 年 5 月 23 日 16:54 UTC

- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMPatchAssociation

描述：提供对子实例的访问权限以进行补丁关联操作。

AmazonSSMPatchAssociation是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMPatchAssociation 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 13 日 16:00 UTC

- 编辑时间：2020 年 5 月 13 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMReadOnlyAccess

描述：提供对 Amazon SSM 的只读访问权限。

AmazonSSMReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSSMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 29 日 17:44 UTC
- 编辑时间：2015 年 5 月 29 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",

```

```
    "ssm:List*"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSSMServiceRolePolicy

描述：提供对 Amazon SSM 管理或使用的 AWS 资源的访问权限

AmazonSSMServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 13 日 19:20 UTC
- 编辑时间：2022 年 9 月 14 日 19:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
    "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSumerianFullAccess

描述：提供对 Amazon Sumerian 的完全访问权限。

AmazonSumerianFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonSumerianFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 24 日 20:14 UTC
- 编辑时间：2018 年 4 月 24 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : [
      "sumerian:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTextractFullAccess

描述：访问所有亚马逊 Textract API

AmazonTextractFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTextractFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 19:07 UTC
- 编辑时间：2018 年 11 月 28 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTextractServiceRole

描述：允许 Textract 代表您呼叫 AWS 服务。

AmazonTextractServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTextractServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 28 日 19:12 UTC
- 编辑时间：2018 年 11 月 28 日 19:12 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamConsoleFullAccess

描述：提供使用管理 Amazon Timestream 的完全访问权限。AWS Management Console 请注意，此策略还向某些 KMS 操作以及管理您保存的查询的操作授予权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

AmazonTimestreamConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTimestreamConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：2022 年 2 月 1 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "kms:EncryptionContextKeys" : "aws:timestream:database-name"
  },
  "Bool" : {
    "kms:GrantIsForAWSResource" : true
  },
  "StringLike" : {
    "kms:ViaService" : "timestream.*.amazonaws.com"
  }
}
},
{
  "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" : "*"    
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamFullAccess

描述：提供对亚马逊 Timestream 的完全访问权限。请注意，此策略还授予某些 KMS 操作访问权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

AmazonTimestreamFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTimestreamFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：2021 年 11 月 26 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
    }  
  ]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamInfluxDBFullAccess

描述：提供创建、更新、删除和列出 Amazon Timestream InfluxDB 实例以及创建和列出参数组的完全管理权限。有关所需的其他权限，请参阅文档。

AmazonTimestreamInfluxDBFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTimestreamInfluxDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 3 月 14 日 22:53
- 编辑时间：世界标准时间 2024 年 3 月 14 日 22:53
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "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"
  ],
  "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::*:*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamInfluxDBServiceRolePolicy

描述：提供创建、更新、删除和列出 Amazon Timestream InfluxDB 实例以及创建和列出参数组的完全管理权限。有关所需的其他权限，请参阅文档。

AmazonTimestreamInfluxDBServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 3 月 14 日 18:53
- 编辑时间：世界标准时间 2024 年 3 月 14 日 18:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamReadOnlyAccess

描述：提供对亚马逊 Timestream 的只读访问权限。策略还提供取消任何正在运行的查询的权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

AmazonTimestreamReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTimestreamReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：世界标准时间 2024 年 6 月 5 日 19:11
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTranscribeFullAccess

描述：提供对 Amazon Transcribe 操作的完全访问权限

AmazonTranscribeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTranscribeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 16:06 UTC
- 编辑时间：2018 年 4 月 4 日 16:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*transcribe*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTranscribeReadOnlyAccess

描述：提供对 Amazon Transcribe 的只读操作的访问权限

AmazonTranscribeReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonTranscribeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 16:05 UTC
- 编辑时间：2018 年 4 月 4 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

描述：提供创建网络接口并将其连接到跨账户资源的权限

AmazonVPCCrossAccountNetworkInterfaceOperations 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCCrossAccountNetworkInterfaceOperations 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 7 月 18 日 20:47 UTC
- 编辑时间：2023 年 9 月 25 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCCrossAccountNetworkInterfaceOperations

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCFullAccess

描述：通过提供对 Amazon VPC 的完全访问权限 AWS Management Console。

AmazonVPCFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 2 月 8 日 16:03
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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: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: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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

描述：提供描述 AWS 资源、运行 Network Access Analyzer 以及在 Network Insights 访问范围和网络见解访问范围分析上创建或删除标签的权限。

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 15 日 22:56 UTC
- 编辑时间：世界标准时间 2024 年 5 月 15 日 21:40
- ARN: arn:aws:iam::aws:policy/
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

描述：提供描述 AWS 资源、运行 Reachability Analyzer 以及在 Network Insights 路径和网络见解分析上创建或删除标签的权限。

AmazonVPCReachabilityAnalyzerFullAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCReachabilityAnalyzerFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 14 日 20:12 UTC
- 编辑时间：世界标准时间 2024 年 5 月 15 日 20:47

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

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "TiroPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
```

```
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

描述：此策略附加到角色 IAM RoleForReachabilityAnalyzerCrossAccountResourceAccess。当管理账户为 Reachability Analyzer 启用可信访问权限时，该角色将部署到组织中的成员账户。该策略提供使用 Reachability Analyzer 控制台查看组织内资源的权限。

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 1 日 20:38 UTC
- 编辑时间：2023 年 5 月 1 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCReadOnlyAccess

描述：通过提供对 Amazon VPC 的只读访问权限 AWS Management Console。

AmazonVPCReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonVPCReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 2 月 8 日 17:08
- ARN: arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkDocsFullAccess

描述：提供 WorkDocs 通过 Amazon 的完全访问权限 AWS Management Console

AmazonWorkDocsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkDocsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 16 日 23:05 UTC
- 编辑时间：2020 年 4 月 16 日 23:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkDocsReadOnlyAccess

描述：WorkDocs 通过提供对 Amazon 的只读访问权限 AWS Management Console

AmazonWorkDocsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkDocsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 8 日 23:49 UTC
- 编辑时间：2020 年 1 月 8 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",

```



```
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkMailEventsServiceRolePolicy

描述：允许访问 Amazon Ev WorkMail ents AWS 服务 及其使用或管理的资源

AmazonWorkMailEventsServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 4 月 16 日 16:52 UTC
- 编辑时间：2019 年 4 月 16 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkMailFullAccess

描述：提供对 Directory Service WorkMail、SES、EC2 的完全访问权限以及对 KMS 元数据的读取权限。

AmazonWorkMailFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkMailFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 12 月 21 日 14:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

策略版本

策略版本：v10（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}

```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkMailMessageFlowFullAccess

描述：对 WorkMail 消息流 API 的完全访问权限

AmazonWorkMailMessageFlowFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkMailMessageFlowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 11 日 11:08 UTC
- 编辑时间：2021 年 2 月 11 日 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkMailMessageFlowReadOnlyAccess

描述：对 GetRawMessageContent API WorkMail 消息的只读访问权限

AmazonWorkMailMessageFlowReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkMailMessageFlowReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 28 日 12:40 UTC
- 编辑时间：2021 年 1 月 28 日 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkMailReadOnlyAccess

描述：提供对 WorkMail 和 SES 的只读访问权限。

AmazonWorkMailReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkMailReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 7 月 25 日 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```


了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesAdmin

描述：提供通过 AWS SDK 和 CLI 访问亚马逊 WorkSpaces 管理操作的权限。

AmazonWorkSpacesAdmin 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkSpacesAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 9 月 22 日 22:21 UTC
- 编辑时间：2023 年 8 月 3 日 23:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Action" : [
  "kms:DescribeKey",
  "kms:ListAliases",
  "kms:ListKeys",
  "workspaces:CreateTags",
  "workspaces:CreateWorkspaceImage",
  "workspaces:CreateWorkspaces",
  "workspaces:CreateStandbyWorkspaces",
  "workspaces>DeleteTags",
  "workspaces:DescribeTags",
  "workspaces:DescribeWorkspaceBundles",
  "workspaces:DescribeWorkspaceDirectories",
  "workspaces:DescribeWorkspaces",
  "workspaces:DescribeWorkspacesConnectionStatus",
  "workspaces:ModifyCertificateBasedAuthProperties",
  "workspaces:ModifySamlProperties",
  "workspaces:ModifyWorkspaceProperties",
  "workspaces:RebootWorkspaces",
  "workspaces:RebuildWorkspaces",
  "workspaces:RestoreWorkspace",
  "workspaces:StartWorkspaces",
  "workspaces:StopWorkspaces",
  "workspaces:TerminateWorkspaces"
],
"Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesApplicationManagerAdminAccess

描述：为在 Amazon WorkSpaces 应用程序管理器中打包应用程序提供管理员访问权限。

AmazonWorkSpacesApplicationManagerAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkSpacesApplicationManagerAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 14:03 UTC
- 编辑时间：2015 年 4 月 9 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonWorkSpacesApplicationManagerAdminAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkspacesPCAAccess

描述：此托管策略提供对 AWS 您中的 Certificate Manager 私有 CA 资源的完全管理权限，AWS 账户以进行基于证书的身份验证。

AmazonWorkspacesPCAAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkspacesPCAAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 8 日 00:25 UTC
- 编辑时间：2022 年 11 月 8 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesSelfServiceAccess

描述：提供对 Amazon WorkSpaces 后端服务的访问权限以执行 Workspace 自助服务操作

AmazonWorkSpacesSelfServiceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkSpacesSelfServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 19:22 UTC
- 编辑时间：2019 年 6 月 27 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesServiceAccess

描述：为客户提供启动工作空间所需的 AWS WorkSpaces 服务的访问权限。

AmazonWorkSpacesServiceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkSpacesServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 19:19 UTC
- 编辑时间：2020 年 3 月 18 日 23:32 UTC

- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesWebReadOnly

描述：通过 AWS Management Console、软件开发工具包和 CLI 提供对 Amazon WorkSpaces Web 及其依赖项的只读访问权限。

AmazonWorkSpacesWebReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmazonWorkSpacesWebReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 30 日 14:20 UTC
- 编辑时间：2022 年 11 月 2 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkSpacesWebServiceRolePolicy

描述：允许 AWS 服务 访问由 Amazon WorkSpaces Web 使用或管理的资源

AmazonWorkSpacesWebServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2021 年 11 月 30 日 13:15 UTC
- 编辑时间 : 2022 年 12 月 15 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonZocaloFullAccess

描述：提供对亚马逊 Zocalo 的完全访问权限。

AmazonZocaloFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonZocaloFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonZocaloReadOnlyAccess

描述：提供对亚马逊 Zocalo 的只读访问权限

AmazonZocaloReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AmazonZocaloReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmplifyBackendDeployFullAccess

描述：提供 Amplify 通过 AWS Cloud 开发套件 (CDK) 部署 Amplify 后端资源（、亚马逊AWS AppSync Cognito、Amazon S3 和其他相关服务）的完全访问权限AWS

AmplifyBackendDeployFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AmplifyBackendDeployFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 10 月 6 日 21:32 UTC
- 编辑时间：世界标准时间 2024 年 5 月 31 日 15:53
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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}"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

APIGatewayServiceRolePolicy

描述：允许 API Gateway 代表客户管理相关 AWS 资源。

APIGatewayServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 17:23 UTC
- 编辑时间：2021 年 7 月 12 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AppIntegrationsServiceLinkedRolePolicy

描述：AppIntegrations 允许代表您管理 AppFlow 资源和发布 CloudWatch 指标数据。

AppIntegrationsServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 30 日 19:42 UTC
- 编辑时间：2022 年 9 月 30 日 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ApplicationAutoScalingForAmazonAppStreamAccess

描述：为 Amazon 启用应用程序自动缩放的策略 AppStream

ApplicationAutoScalingForAmazonAppStreamAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ApplicationAutoScalingForAmazonAppStreamAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 2 月 6 日 21:39 UTC
- 编辑时间：2017 年 2 月 6 日 21:39 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

描述：允许访问由 ApplicationDiscoveryService 持续导出功能使用或管理的资源

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 9 日 20:22 UTC
- 编辑时间：2018 年 8 月 13 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AppRunnerNetworkingServiceRolePolicy

描述：允许 AWS AppRunner 网络代表您管理相关 AWS 资源。

AppRunnerNetworkingServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 1 月 12 日 21:02 UTC
- 编辑时间：2022 年 1 月 12 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AppRunnerServiceRolePolicy

描述：AWS AppRunner 允许代表您管理相关 AWS 资源。

AppRunnerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 14 日 19:15 UTC
- 编辑时间：2021 年 5 月 14 日 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingConsoleFullAccess

描述：通过提供对 Auto Scaling 的完全访问权限 AWS Management Console。

AutoScalingConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AutoScalingConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:43 UTC
- 编辑时间：2018 年 2 月 6 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingConsoleReadOnlyAccess

描述：通过提供对 Auto Scaling 的只读访问权限 AWS Management Console。

AutoScalingConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AutoScalingConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:48 UTC
- 编辑时间：2017 年 1 月 12 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingFullAccess

描述：提供对 Auto Scaling 的完全访问权限。

AutoScalingFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AutoScalingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:31 UTC
- 编辑时间：2018 年 2 月 6 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingNotificationAccessRole

描述：AutoScaling 通知访问服务角色的默认策略。

AutoScalingNotificationAccessRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AutoScalingNotificationAccessRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
        "sqs:GetQueueUrl",
        "sns:Publish"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingReadOnlyAccess

描述：提供对 Auto Scaling 的只读访问权限。

AutoScalingReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AutoScalingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:39 UTC
- 编辑时间：2017 年 1 月 12 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AutoScalingServiceRolePolicy

描述：允许 AWS 服务 访问由 Auto Scaling 使用或管理的资源

AutoScalingServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 1 月 8 日 23:10 UTC
- 编辑时间：世界标准时间 2024 年 2 月 29 日 17:48
- ARN: arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWS_ConfigRole

描述：AWS Config 服务角色的默认策略。提供 AWS Config 跟踪 AWS 资源更改所需的权限。

AWS_ConfigRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWS_ConfigRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 15 日 20:30 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 21:19
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

策略版本

策略版本：v30 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"apigateway:GET",
"app-integrations:GetEventIntegration",
"app-integrations:ListEventIntegrationAssociations",
"app-integrations:ListEventIntegrations",
"appconfig:GetApplication",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetExtensionAssociation",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"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: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",
"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:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch: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",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"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",
"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",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config:Select*",
```

```
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
"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",
"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",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"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:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"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",
"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:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"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",
"finespace:GetEnvironment",
"finespace: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:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTags",
"glue:GetWorkflow",
"glue:ListCrawlers",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"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",
"imagebuilder:GetComponent",
"imagebuilder:GetContainerRecipe",
"imagebuilder:GetDistributionConfiguration",
"imagebuilder:GetImage",
"imagebuilder:GetImagePipeline",
"imagebuilder:GetImageRecipe",
"imagebuilder:GetInfrastructureConfiguration",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"inspector2:BatchGetAccountStatus",
"inspector2:GetDelegatedAdminAccount",
"inspector2:ListFilters",
"inspector2:ListMembers",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuthorizer",
"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:GetPolicy",
"iot:GetTopicRule",
"iot:GetTopicRuleDestination",
"iot:ListAuthorizers",
"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: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",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"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:GetFuotaTask",
"iotwireless:GetMulticastGroup",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamKey",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreamKeys",
"ivs: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:GetFunction",
"lambda:GetFunctionCodeSigningConfig",
"lambda:GetLayerVersion",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"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:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:GetDataProtectionPolicy",
"logs:GetLogDelivery",
"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:ListCustomDataIdentifiers",
"macie2:ListTagsForResource",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNodes",
"mediaconnect:DescribeFlow",
"mediaconnect:ListFlows",
"mediaconnect:ListTagsForResource",
"mediapackage-vod:DescribePackagingConfiguration",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mediapackage-vod:ListTagsForResource",
"mediatailor:GetPlaybackConfiguration",
"mediatailor:ListPlaybackConfigurations",
"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:GetTransitGatewayRegistrations",
"networkmanager:ListConnectPeers",
"networkmanager:ListTagsForResource",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetStreamingImage",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStudioComponents",
"nimble:ListStudios",
"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",
"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",
"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:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"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:DescribeLoggingStatus",
"redshift:DescribeScheduledActions",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"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",
"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: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:ListAccessPoints",
"s3:ListAccessPointsForObjectLambda",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"s3:ListStorageLensConfigurations",
"s3express:GetBucketPolicy",
"s3express:ListAllMyDirectoryBuckets",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceExperiment",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribeProject",
"sagemaker:DescribeWorkteam",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListCodeRepositories",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDomains",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListFeatureGroups",
"sagemaker:ListImages",
"sagemaker:ListImageVersions",
"sagemaker:ListInferenceExperiments",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
```

```
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelines",
"sagemaker:ListProjects",
"sagemaker:ListTags",
"sagemaker:ListWorkteams",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"sdb:GetAttributes",
"sdb:ListDomains",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:DescribeHub",
"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:GetEmailTemplate",
"ses:GetTemplate",
"ses:ListConfigurationSets",
"ses:ListContactLists",
"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:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:DescribeDocumentPermission",
"ssm:DescribeParameters",
"ssm:GetAutomationExecution",
"ssm:GetDocument",
"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",
"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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAccountActivityAccess

描述：允许用户访问账户活动页面。

AWSAccountActivityAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAccountActivityAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2015 年 2 月 6 日 18:41 UTC
- 编辑时间 : 2023 年 3 月 7 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAccountManagementFullAccess

描述：提供对 AWS 账户管理的完全访问权限。

AWSAccountManagementFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAccountManagementFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 30 日 23:20 UTC
- 编辑时间：2021 年 9 月 30 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "account:*",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAccountManagementReadOnlyAccess

描述：提供对 AWS 账户管理的只读访问权限

AWSAccountManagementReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAccountManagementReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 30 日 23:29 UTC
- 编辑时间：2021 年 9 月 30 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAccountUsageReportAccess

描述：允许用户访问账户使用情况报告页面。

AWSAccountUsageReportAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAccountUsageReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAgentlessDiscoveryService

描述：为 Discovery 无代理连接器提供向 Application Discovery Service 注册的 AWS 访问权限。

AWSAgentlessDiscoveryService 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSAgentlessDiscoveryService` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 8 月 2 日 01:35 UTC
- 编辑时间：2020 年 2 月 24 日 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppFabricFullAccess

描述：提供对服务的完全访问权限和对依赖 AWS AppFabric 服务（例如 S3、Kinesis、KMS）的只读访问权限。

AWSAppFabricFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppFabricFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 19:51 UTC
- 编辑时间：2023 年 6 月 27 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppFabricReadOnlyAccess

描述：提供对的只读访问权限 AWS AppFabric

AWSAppFabricReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSAppFabricReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 19:52 UTC

- 编辑时间：2023 年 6 月 27 日 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppFabricServiceRolePolicy

描述：代表您 AppFabric 访问 AWS 资源

AWSAppFabricServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 26 日 21:07 UTC
- 编辑时间：2023 年 6 月 26 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

描述：授予 Application Auto Scaling 访问 AppStream 和的权限的策略 CloudWatch。

AWSApplicationAutoscalingAppStreamFleetPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 19:04 UTC
- 编辑时间：2017 年 10 月 20 日 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingCassandraTablePolicy

描述：向应用程序 Auto Scaling 授予访问 Cassandra 和 CloudWatch。

AWSApplicationAutoscalingCassandraTablePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 3 月 18 日 22:49 UTC
- 编辑时间：2020 年 3 月 18 日 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

描述：授予 Application Auto Scaling 访问权限 Comprehend 和 CloudWatch

AWSApplicationAutoscalingComprehendEndpointPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 14 日 18:39 UTC
- 编辑时间：2019 年 11 月 14 日 18:39 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoScalingCustomResourcePolicy

描述 : 授予 Application Auto Scaling 访问 ApigateWay 和自定义资源扩展权限 CloudWatch 的策略

AWSApplicationAutoScalingCustomResourcePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 4 日 23:22 UTC
- 编辑时间：2018 年 6 月 4 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

描述：向应用程序 Auto Scaling 授予访问 DynamoDB 和 CloudWatch

AWSApplicationAutoscalingDynamoDBTablePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 21:34 UTC
- 编辑时间：2017 年 10 月 20 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "Action" : [
      "dynamodb:DescribeTable",
      "dynamodb:UpdateTable",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

描述：向应用程序 Auto Scaling 授予访问 EC2 Spot 队列和 CloudWatch。

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 25 日 18:23 UTC
- 编辑时间：2017 年 10 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingECSServicePolicy

描述：向应用程序 Auto Scaling 授予访问 EC2 容器服务的权限的策略，以及 CloudWatch。

AWSApplicationAutoscalingECSServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 25 日 23:53 UTC
- 编辑时间：2017 年 10 月 25 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingElastiCacheRGPoicy

描述：授予应用程序 Auto Scaling 访问亚马逊 ElastiCache 和亚马逊的权限的策略 CloudWatch。

AWSApplicationAutoscalingElastiCacheRGPoicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 17 日 23:41 UTC
- 编辑时间：2021 年 8 月 17 日 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPoicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
```

```
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeCacheParameters",
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

描述：向 Application Auto Scaling 授予访问 Elastic Map Reduce 和 CloudWatch。

AWSApplicationAutoscalingEMRInstanceGroupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 26 日 00:57 UTC

- 编辑时间：2017 年 10 月 26 日 00:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingKafkaClusterPolicy

描述：授予应用程序 Auto Scaling 访问适用于 Apache Managed Kafka 的托管流媒体的权限的策略
CloudWatch

AWSApplicationAutoscalingKafkaClusterPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 24 日 18:36 UTC
- 编辑时间：2020 年 8 月 24 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

描述：授予应用程序 Auto Scaling 访问 Lambda 和 CloudWatch 的权限的策略。

AWSApplicationAutoscalingLambdaConcurrencyPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 21 日 20:04 UTC
- 编辑时间：2019 年 10 月 21 日 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:PutProvisionedConcurrencyConfig",
      "lambda:GetProvisionedConcurrencyConfig",
      "lambda>DeleteProvisionedConcurrencyConfig",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

描述：授予应用程序 Auto Scaling 访问亚马逊 Neptune 和亚马逊权限的策略。 CloudWatch

AWSApplicationAutoscalingNeptuneClusterPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 2 日 21:14 UTC
- 编辑时间：2021 年 9 月 2 日 21:14 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingRDSClusterPolicy

描述：授予 Application Auto Scaling 访问权限的策略，以访问 RDS 和 CloudWatch。

AWSApplicationAutoscalingRDSClusterPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 17 日 17:46 UTC
- 编辑时间：2018 年 8 月 7 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

描述：授予 Application Auto Scaling 访问 SageMaker 和的权限的策略 CloudWatch。

AWSApplicationAutoscalingSageMakerEndpointPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 2 月 6 日 19:58 UTC
- 编辑时间：2023 年 11 月 13 日 18:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationDiscoveryAgentAccess

描述：为 Discovery 代理提供向 App AWS lication Discovery Service 注册的权限。

AWSApplicationDiscoveryAgentAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationDiscoveryAgentAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 5 月 11 日 21:38 UTC
- 编辑时间：2020 年 2 月 24 日 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

描述：允许 Application Discovery Service 无代理收集器自动更新、注册和与应用程序发现服务通信

AWSApplicationDiscoveryAgentlessCollectorAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationDiscoveryAgentlessCollectorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 16 日 21:00 UTC
- 编辑时间：2022 年 8 月 16 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationDiscoveryAgentlessCollectorAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationDiscoveryServiceFullAccess

描述：提供查看和标记由 App AWS lication Discovery Service 维护的配置项目的完全访问权限

AWSApplicationDiscoveryServiceFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationDiscoveryServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 5 月 11 日 21:30 UTC
- 编辑时间：2019 年 6 月 19 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationAgentInstallationPolicy

描述：此策略允许安装 AWS 复制代理，该代理与 AWS 应用程序迁移服务 (MGN) 一起使用，用于将外部服务器迁移到。AWS 将此策略附加到您在安装 AWS 复制代理时提供其证书的 IAM 用户或角色。

AWSApplicationMigrationAgentInstallationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationAgentInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 6 月 19 日 07:51 UTC

- 编辑时间 : 2022 年 9 月 20 日 11:21 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationAgentInstallationPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationAgentPolicy

描述：此策略允许安装和使用 AWS 复制代理，该代理与 AWS 应用程序迁移服务 (MGN) 一起使用，用于将外部服务器迁移到。AWS 将此策略附加到您在安装 AWS 复制代理时提供其证书的 IAM 用户或角色。

AWSApplicationMigrationAgentPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationAgentPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 07:00 UTC
- 编辑时间：2022 年 9 月 20 日 11:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationAgentPolicy_v2

描述：此策略允许使用 AWS 复制代理，该代理与 AWS 应用程序迁移服务 (MGN) 一起使用，将外部服务器迁移到。AWS 我们不建议您将此策略附加到 IAM 用户或角色。

AWSApplicationMigrationAgentPolicy_v2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationAgentPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 6 月 6 日 14:14 UTC
- 编辑时间：2022 年 6 月 6 日 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
  }
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationConversionServerPolicy

描述：此策略允许应用程序迁移服务 (MGN) 转换服务器 (由应用程序迁移服务启动的 EC2 实例) 与 MGN 服务通信。MGN 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 MGN 转换服务器，由 MGN 在需要时自动启动和终止。我们不建议您将此策略附加到您的 IAM 用户或角色。当用户选择使用 MGN 控制台、CLI 或 API 启动测试或割接实例时，Application Migration Service 会使用 MGN 转换服务器。

AWSApplicationMigrationConversionServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationConversionServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 06:48 UTC
- 编辑时间：2021 年 4 月 7 日 06:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationEC2Access

描述：此策略提供使用应用程序迁移服务 (MGN) 将迁移的服务器作为 EC2 实例启动所需的 Amazon EC2 操作。可将此策略附加到您的 IAM 用户或角色。

AWSApplicationMigrationEC2Access 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 07:05 UTC
- 编辑时间：2023 年 2 月 6 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ],
  "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"
      }
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationFullAccess

描述：此策略为 AWS 应用程序迁移服务 (MGN) 的所有公共 API 提供权限，以及读取 KMS 密钥信息的权限。可将此策略附加到您的 IAM 用户或角色。

AWSApplicationMigrationFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 06:56 UTC
- 编辑时间：世界标准时间 2024 年 5 月 19 日 08:30

- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*: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"

```

```
    ]
  }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationMGHAccess

描述：此策略允许 AWS 应用程序迁移服务 (MGN) 将有关使用 MGN 的服务器迁移进度的元数据发送到 Migration Hub (MG AWS H)。MGN 会自动创建附加此策略的 IAM 角色，并使用该角色。我们不建议您将此策略附加到 IAM 用户或角色。

AWSApplicationMigrationMGHAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationMGHAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 07:10 UTC
- 编辑时间：2021 年 4 月 7 日 07:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationReadOnlyAccess

描述：此策略为应用程序迁移服务 (MGN) 的所有只读公共 API 以及其他 AWS 服务的一些只读 API 提供权限，这些 API 是完全只读使用 MGN 控制台所必需的。可将此策略附加到您的 IAM 用户或角色。

AWSApplicationMigrationReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSApplicationMigrationReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 07:15 UTC
- 编辑时间：2023 年 3 月 20 日 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationReplicationServerPolicy

描述：此策略允许应用程序迁移服务 (MGN) 复制服务器（由应用程序迁移服务启动的 EC2 实例）与 MGN 服务通信，并在您的中创建 EBS 快照。AWS 账户 Application Migration Service 将具有此策略的 IAM 角色（作为 EC2 实例配置文件）附加到 MGN 复制服务器，这些服务器将由 MGN 按需自动启动和终止。作为使用 MGN 管理的迁移过程的一部分 AWS，MGN 复制服务器用于促进从外部服务器向其复制数据。我们不建议您将此策略附加到 IAM 用户或角色。

AWSApplicationMigrationReplicationServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationReplicationServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 07:21 UTC
- 编辑时间：2021 年 4 月 7 日 07:21 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationServiceEc2InstancePolicy

描述：此策略允许安装和使用 AWS 复制代理，AWS 应用程序迁移服务 (AWS MGN) 使用它来迁移在 EC2 (跨区域或跨可用区) 上运行的源服务器。应将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 EC2 实例。

AWSApplicationMigrationServiceEc2InstancePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationServiceEc2InstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 22 日 13:19 UTC
- 编辑时间：世界标准时间 2024 年 1 月 3 日 14:19
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationServiceEc2InstancePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationServiceRolePolicy

描述：允许 AWS 应用程序迁移服务代表您创建和管理 AWS 资源。

AWSApplicationMigrationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 7 日 06:43 UTC
- 编辑时间：2023 年 6 月 20 日 09:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate",
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      }
    }
  }
}
```

```
    }  
  ]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationSSMAccess

描述：此策略允许访问使用应用程序迁移服务 (MGN) 执行自定义迁移后命令 SSM 文档所需的 Amazon SSM 操作。可将此策略附加到您的 IAM 用户或角色。

AWSApplicationMigrationSSMAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationSSMAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 09:29 UTC
- 编辑时间：2023 年 3 月 20 日 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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-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/*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSApplicationMigrationVCenterClientPolicy

描述：此策略允许安装和使用 AWS vCenter Client，该客户端与 AWS 应用程序迁移服务 (MGN) 一起使用，用于将外部服务器迁移到。AWS 将此策略附加到您在安装 AWS vCenter 客户端时提供其证书的 IAM 用户或角色。

AWSApplicationMigrationVCenterClientPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSApplicationMigrationVCenterClientPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 8 日 12:53 UTC
- 编辑时间：2021 年 11 月 8 日 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshEnvoyAccess

描述：用于访问虚拟节点配置的 App Mesh Envoy 策略。

AWSAppMeshEnvoyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppMeshEnvoyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 3 日 21:29 UTC

- 编辑时间：2019 年 7 月 3 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshFullAccess

描述：提供对 AWS App Mesh API 和管理控制台的完全访问权限。

AWSAppMeshFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSAppMeshFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 16 日 17:50 UTC
- 编辑时间：2021 年 1 月 7 日 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshPreviewEnvoyAccess

描述：用于访问虚拟节点配置的 App Mesh Preview Envoy 策略。

AWSAppMeshPreviewEnvoyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppMeshPreviewEnvoyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 8 月 5 日 23:32 UTC
- 编辑时间：2019 年 8 月 5 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshPreviewServiceRolePolicy

描述：允许访问 App Mesh AWS 服务 以及由 AWS App Mesh 使用或管理的资源

AWSAppMeshPreviewServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 19 日 19:07 UTC
- 编辑时间：2019 年 8 月 21 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CloudMapServiceDiscovery",
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:DiscoverInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ACMCertificateVerification",
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshReadOnly

描述：提供对 AWS App Mesh API 和管理控制台的只读访问权限。

AWSAppMeshReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSAppMeshReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 16 日 17:51 UTC

- 编辑时间：2021 年 1 月 7 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppMeshServiceRolePolicy

描述：允许访问 AWS 服务 以及由其使用或管理的资源 AWS AppMesh

AWSAppMeshServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 3 日 18:30 UTC
- 编辑时间：2023 年 10 月 10 日 16:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppRunnerFullAccess

描述：授予所有 App Runner 操作的权限。

AWSAppRunnerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSAppRunnerFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 1 月 11 日 04:02 UTC
- 编辑时间：2022 年 1 月 11 日 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppRunnerReadOnlyAccess

描述：授予列出和查看 App Runner 资源详细信息的权限。

AWSAppRunnerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppRunnerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 2 月 24 日 21:24 UTC
- 编辑时间：2022 年 2 月 24 日 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppRunnerServicePolicyForECRAccess

描述：AWS App Runner 服务政策，授予对客户账户中的 Amazon ECR 资源的读取权限。可在创建或更新 App Runner 服务时传递给 App Runner 的角色中使用该策略。

AWSAppRunnerServicePolicyForECRAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppRunnerServicePolicyForECRAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 5 月 14 日 19:17 UTC
- 编辑时间：2021 年 5 月 14 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppSyncAdministrator

描述：提供对 AppSync 服务的管理访问权限，但还不足以通过控制台进行访问。

AWSAppSyncAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppSyncAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:20 UTC
- 编辑时间：2019 年 11 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppSyncInvokeFullAccess

描述：通过控制台和独立提供对 AppSync 服务的完全调用访问权限

AWSAppSyncInvokeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppSyncInvokeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:21 UTC
- 编辑时间：2018 年 3 月 20 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppSyncPushToCloudWatchLogs

描述：AppSync 允许将日志推送到用户的 CloudWatch 账户。

AWSAppSyncPushToCloudWatchLogs 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppSyncPushToCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 4 月 9 日 19:38 UTC
- 编辑时间：2018 年 4 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppSyncSchemaAuthor

描述：提供创建、更新和查询架构的权限。

AWSAppSyncSchemaAuthor 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSAppSyncSchemaAuthor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:21 UTC
- 编辑时间：2023 年 2 月 1 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAppSyncServiceRolePolicy

描述：允许访问由其使用或管理的 AWS 服务和资源 AppSync

AWSAppSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 1 月 21 日 19:56 UTC
- 编辑时间：2020 年 1 月 21 日 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSArtifactAccountSync

描述：允许 A AWS rtifact 对 AWS 组织中的操作进行只读访问。

AWSArtifactAccountSync是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSArtifactAccountSync 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2018 年 4 月 10 日 23:04 UTC
- 编辑时间：2018 年 4 月 10 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSArtifactReportsReadOnlyAccess

描述：提供对 Artifact 服务 AWS 报告的只读访问权限。

AWSArtifactReportsReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSArtifactReportsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 1 月 2 日 22:42
- 编辑时间：世界标准时间 2024 年 1 月 2 日 22:42
- ARN: arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSArtifactServiceRolePolicy

描述：允许 A AWS rtifact 通过 Organizations 服务收集有关 AWS 组织的信息。

AWSArtifactServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 8 月 21 日 20:27 UTC
- 编辑时间：2023 年 8 月 21 日 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListAccounts",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAuditManagerAdministratorAccess

描述：提供管理权限以启用或禁用 Au AWS dit Manager、更新设置以及管理评估、控件和框架

AWSAuditManagerAdministratorAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSAuditManagerAdministratorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 11 日 20:02 UTC
- 编辑时间：世界标准时间 2024 年 5 月 15 日 23:46
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAuditManagerServiceRolePolicy

描述：允许访问 Audit Manager AWS 服务 以及由 Audit Manager 使用或 AWS 管理的资源

AWSAuditManagerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 8 日 15:12 UTC
- 编辑时间：世界标准时间 2024 年 6 月 10 日 20:28
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

描述：该策略授予 AWS Auto Scaling 定期预测容量并为扩展计划中的 Auto Scaling 组生成计划扩展操作的权限

AWSAutoScalingPlansEC2AutoScalingPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 23 日 22:46 UTC
- 编辑时间：2018 年 8 月 23 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupAuditAccess

描述：此策略允许用户创建控制和框架，以定义他们对 AWS 备份资源和活动的期望，并根据其定义的控制和框架审计 AWS Backup 资源和活动。此政策向 AWS Config 和类似服务授予权限，以描述用户期望执行审计。此策略还向 S3 和类似服务授予提供审计报告的权限，并使用户能够查找和打开其审计报告。

AWSBackupAuditAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupAuditAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 24 日 01:02 UTC
- 编辑时间：2023 年 4 月 10 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:::*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupDataTransferAccess

描述：此策略允许 AWS Backint 代理使用 Backup Storage 平面完成 AWS 备份数据传输。将此策略附加到使用 Backint Agent 运行 SAP HANA 的 EC2 实例所具有的角色。

AWSBackupDataTransferAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupDataTransferAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 22:48 UTC
- 编辑时间：2022 年 11 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupFullAccess

描述：此策略适用于备份管理员，授予对 AWS 备份操作的完全访问权限，包括创建或编辑备份计划、为备份计划分配 AWS 资源、删除备份和恢复备份。

AWSBackupFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 18 日 22:21 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 17:33
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

策略版本

策略版本 : v17 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListVolumes",
    "storagegateway:ListLocalDisks"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
},
{
  "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" : "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

描述：提供代表您同步虚拟机元数据的 AWS BackupGateway 权限

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 12 月 15 日 19:43 UTC
- 编辑时间：2022 年 12 月 15 日 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupOperatorAccess

描述：此策略授予用户为备份计划分配 AWS 资源、创建按需备份和还原备份的权限。此策略不允许用户创建或编辑备份计划，也不允许用户在创建计划备份之后删除这些备份。

AWSBackupOperatorAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupOperatorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 18 日 22:23 UTC

- 编辑时间：2023 年 9 月 6 日 20:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup>DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob"
      ],
      "Resource" : "*"
    },
    {
      "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFilesystems"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetTagKeys",
```

```
    "tag:GetTagValues",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeCachediSCSIVolumes",
    "storagegateway:DescribeStorediSCSIVolumes"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:ListGateways"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "storagegateway:DescribeGatewayInformation",
    "storagegateway:ListVolumes",
    "storagegateway:ListLocalDisks"
  ],
  "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam:*:*:role/*AwsBackup*",
    "arn:aws:iam:*:*:role/*AWSBackup*"
  ]
},
```

```
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "backup.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "organizations:DescribeOrganization",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "fsx:DescribeBackups",
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "fsx:DescribeFileSystems",
    "Resource" : "arn:aws:fsx:*:*:file-system/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "fsx:DescribeVolumes",
    "Resource" : "arn:aws:fsx:*:*:volume/*/*"
  },
  {
    "Effect" : "Allow",
```



```
    "Action" : "fsx:DescribeStorageVirtualMachines",
    "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ds:DescribeDirectories",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:ListGateways",
      "backup-gateway:ListHypervisors",
      "backup-gateway:ListTagsForResource",
      "backup-gateway:ListVirtualMachines"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetHypervisor",
      "backup-gateway:GetHypervisorPropertyMappings"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetVirtualMachine"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-gateway:GetBandwidthRateLimitSchedule",
      "backup-gateway:GetGateway"
    ],
    "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:GetMetricData",
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "timestream:ListDatabases",
      "timestream:ListTables"
    ],
    "Resource" : [
      "arn:aws:timestream:*:*:database/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "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:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
    "redshift:DescribeNodeConfigurationOptions",
    "redshift:DescribeOrderableClusterOptions",
    "redshift:DescribeClusterParameterGroups",
    "redshift:DescribeClusterTracks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStacks"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetOperation",
    "ssm-sap:ListDatabases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetDatabase",
    "ssm-sap:ListTagsForResource"
  ],
  "Resource" : "arn:aws:ssm-sap:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupOrganizationAdminAccess

描述：此政策适用于使用跨账户备份管理来管理组织备份的备份管理员。

AWSBackupOrganizationAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupOrganizationAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 16:23 UTC
- 编辑时间：2022 年 11 月 18 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupRestoreAccessForSAPHANA

描述：提供 AWS 备份权限，用于在亚马逊 EC2 上恢复 SAP HANA 的备份

AWSBackupRestoreAccessForSAPHANA是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSBackupRestoreAccessForSAPHANA` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 22:43 UTC
- 编辑时间：2022 年 11 月 10 日 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceLinkedRolePolicyForBackup

描述：提供 AWS Backup 权限，允许您代表您跨 AWS 服务创建备份

AWSBackupServiceLinkedRolePolicyForBackup 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 2 日 23:08 UTC
- 编辑时间：世界标准时间 2024 年 5 月 17 日 17:12

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

策略版本

策略版本 : v16 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "RDSInstanceAndSnapshotPermissions",
```

```
"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" : "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" : "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}"
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

描述：提供 AWS Backup 权限，允许您代表您跨 AWS 服务创建备份

AWSBackupServiceLinkedRolePolicyForBackupTest 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 5 月 12 日 17:37 UTC
- 编辑时间：2020 年 5 月 12 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceRolePolicyForBackup

描述：提供 AWS Backup 权限，允许您代表您跨 AWS 服务创建备份

AWSBackupServiceRolePolicyForBackup 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSBackupServiceRolePolicyForBackup` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 10 日 21:01 UTC
- 编辑时间：世界标准时间 2024 年 5 月 17 日 17:12
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

策略版本

策略版本：v19 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "RDSModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:ModifyDBInstance"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:db:*"
    ]
  },
  {
    "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" : "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" : "KMSSDataKeyEC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com"
      ]
    }
  }
},
{
  "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" : "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}"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceRolePolicyForRestores

描述：提供 AWS Backup 权限，允许您代表您跨 AWS 服务执行恢复。此策略包括创建和删除 AWS 资源（例如 EBS 卷、RDS 实例和 EFS 文件系统）的权限，这些资源是恢复过程的一部分。

AWSBackupServiceRolePolicyForRestores 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupServiceRolePolicyForRestores 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 12 日 00:23 UTC

- 编辑时间：世界标准时间 2023 年 12 月 15 日 22:05
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores

策略版本

策略版本：v20（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : "*"
},
{
  "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"
  ],
  "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" : "KMSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "dynamodb.*.amazonaws.com",
        "ec2.*.amazonaws.com",
        "elasticfilesystem.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "redshift.*.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" : {
      "ForAnyValue: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:*"
  ]
},
{
  "Sid" : "RedshiftClusterPermissions",
```

```
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:cluster:*"
    ]
  },
  {
    "Sid" : "RedshiftTablePermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeTableRestoreStatus"
    ],
    "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" : [
      "*"
    ]
  }
]
```



```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceRolePolicyForS3Backup

描述：包含 AWS Backup 在任何 S3 存储桶中备份数据所需的权限的策略。其中包括对所有 S3 对象的读取权限以及所有 KMS 密钥的全部解密访问权限。

AWSBackupServiceRolePolicyForS3Backup 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupServiceRolePolicyForS3Backup 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 2 月 18 日 17:40 UTC
- 编辑时间：世界标准时间 2024 年 5 月 17 日 17:12
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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}"
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBackupServiceRolePolicyForS3Restore

描述：包含 Backup 将 S3 AWS 备份还原到存储桶所需的权限的策略。这包括所有 S3 存储桶的读/写权限，以及所有 KMS 密钥 DescribeKey 的读/写权限。GenerateDataKey

AWSBackupServiceRolePolicyForS3Restore 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBackupServiceRolePolicyForS3Restore 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 2 月 18 日 17:39 UTC
- 编辑时间：2023 年 2 月 7 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBatchFullAccess

描述：提供对 Batch AWS 资源的完全访问权限。

AWSBatchFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBatchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 6 日 19:35 UTC
- 编辑时间：2022 年 10 月 24 日 16:09 UTC

- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBatchServiceEventTargetRole

描述：用于为 B AWS atch Job 提交启用 CloudWatch 事件目标的策略

AWSBatchServiceEventTargetRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSBatchServiceEventTargetRole` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 2 月 28 日 22:31 UTC
- 编辑时间：2018 年 2 月 28 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBatchServiceRole

描述：Batch AWS h 服务角色策略，允许访问相关服务，包括 EC2、Autoscaling、EC2 容器服务和 Cloudwatch 日志。

AWSBatchServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBatchServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 6 日 19:36 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 18:49
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBCMDataExportsServiceRolePolicy

描述：一个服务关联角色，用于为账单和成本管理数据导出提供访问 AWS 服务数据的权限，以便代表客户将数据导出到目标位置，例如 Amazon S3。

AWSBCMDataExportsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 6 月 10 日 17:40
- 编辑时间：世界标准时间 2024 年 6 月 10 日 17:40
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBillingConductorFullAccess

描述：使用 AWSBillingConductorFullAccess 托管策略允许完全访问 AWS Billing Conductor (ABC) 控制台和 API。此策略允许用户列出、创建和删除 ABC 资源。

AWSBillingConductorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBillingConductorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 13 日 18:02 UTC
- 编辑时间：2022 年 4 月 13 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "billingconductor:*",
      "organizations:ListAccounts",
      "pricing:DescribeServices"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBillingConductorReadOnlyAccess

描述：使用 `AWSBillingConductorReadOnlyAccess` 托管策略允许对 AWS Billing Conductor (ABC) 控制台和 API 进行只读访问。此策略授予权限，使其能够查看和列出所有 ABC 资源。它不包括创建或删除资源的能力。

`AWSBillingConductorReadOnlyAccess` 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSBillingConductorReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 13 日 18:02 UTC
- 编辑时间：2022 年 4 月 13 日 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBillingReadOnlyAccess

描述：允许用户在账单控制台上查看账单。

AWSBillingReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBillingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 27 日 20:08 UTC
- 编辑时间：世界标准时间 2024 年 5 月 23 日 23:23
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetInvoiceEmailDeliveryPreferences",
"invoicing:GetInvoicePDF",
"invoicing:ListInvoiceSummaries",
"payments:GetPaymentInstrument",
"payments:GetPaymentStatus",
"payments:ListPaymentPreferences",
"payments:ListTagsForResource",
"payments:ListPaymentInstruments",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:ViewPurchaseOrders",
"purchase-orders:ListPurchaseOrderInvoices",
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ListTagsForResource",
"sustainability:GetCarbonFootprintSummary",
"tax:GetTaxRegistrationDocument",
"tax:GetTaxInheritance",
"tax:ListTaxRegistrations"
],
"Resource" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

描述：此策略授予控制 AWS 资源的权限。例如，通过执行 S AWS systems Manager (SSM) 脚本来启动和停止 EC2 或 RDS 实例。

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 5 月 25 日 19:03 UTC
- 编辑时间：2022 年 5 月 25 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBudgetsActionsWithAWSResourceControlAccess

描述：提供对 AWS 预算操作的完全访问权限，包括使用预算操作通过以下方式控制 AWS 资源的运行状态 AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBudgetsActionsWithAWSResourceControlAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 15 日 17:19 UTC
- 编辑时间：2020 年 10 月 15 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActionsWithAWSResourceControlAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBudgetsReadOnlyAccess

描述：通过提供对 AWS 预算控制台的只读访问权限 AWS Management Console。

AWSBudgetsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBudgetsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 15 日 17:18 UTC
- 编辑时间：2020 年 10 月 15 日 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ]
    }
  ]
}
```



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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBugBustFullAccess

描述：此 IAM 策略授予用户对 AWS BugBust 控制台的完全访问权限

AWSBugBustFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBugBustFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 6 月 24 日 07:03 UTC
- 编辑时间：2021 年 7 月 22 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBugBustPlayerAccess

描述：此 IAM 策略授予用户参与 AWS BugBust 活动的权限

AWSBugBustPlayerAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSBugBustPlayerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 6 月 24 日 07:15 UTC
- 编辑时间：2021 年 6 月 24 日 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSBugBustServiceRolePolicy

描述：授予代表您访问资源的权限 AWS BugBust

AWSBugBustServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 24 日 06:59 UTC
- 编辑时间：2021 年 6 月 24 日 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",

```

```
    "codeguru-reviewer:DescribeCodeReview"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/bugbust" : "enabled"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerFullAccess

描述：提供对 Certificate Manager (ACM) 的完全访问权限

AWSCertificateManagerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 21 日 17:02 UTC
- 编辑时间：2020 年 8 月 17 日 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerPrivateCAAuditor

描述：为审核员提供对 Certificate Manager 私有证书颁发机构的访问权限

AWSCertificateManagerPrivateCAAuditor 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerPrivateCAAuditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:51 UTC
- 编辑时间：2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerPrivateCAFullAccess

描述：提供对 Certificate Manager 私有 AWS 证书颁发机构的完全访问权限

AWSCertificateManagerPrivateCAFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerPrivateCAFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 10 月 23 日 16:54 UTC
- 编辑时间：2018 年 10 月 23 日 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerPrivateCAPrivilegedUser

描述：为特权证书用户提供对 Certificate Manager 私有证书颁发机构的访问权限 AWS

AWSCertificateManagerPrivateCAPrivilegedUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSCertificateManagerPrivateCAPrivilegedUser` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 20 日 17:43 UTC
- 编辑时间：2019 年 6 月 20 日 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
```

```
    "acm-pca:IssueCertificate"
  ],
  "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
  "Condition" : {
    "StringNotLike" : {
      "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerPrivateCAReadOnly

描述：提供对 Certificate Manager 私有 AWS 证书颁发机构的只读访问权限

AWSCertificateManagerPrivateCAReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerPrivateCAReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:57 UTC
- 编辑时间：2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerPrivateCAUser

描述：为证书用户提供对 Certificate Manager 私有证书颁发机构的访问权限 AWS

AWSCertificateManagerPrivateCAUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerPrivateCAUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:53 UTC
- 编辑时间：2019 年 6 月 20 日 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Action" : [
  "acm-pca:IssueCertificate"
],
"Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
"Condition" : {
  "StringLike" : {
    "acm-pca:TemplateArn" : [
      "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
    ]
  }
}
},
{
  "Effect" : "Deny",
  "Action" : [
    "acm-pca:IssueCertificate"
  ],
  "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
  "Condition" : {
    "StringNotLike" : {
      "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" : "*"
}
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCertificateManagerReadOnly

描述：提供对 Certificate Manager (ACM) 的只读访问权限。

AWSCertificateManagerReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCertificateManagerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 21 日 17:07 UTC
- 编辑时间：2021 年 3 月 15 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



```
"Version" : "2012-10-17",
"Statement" : {
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate",
    "acm:ListCertificates",
    "acm:GetCertificate",
    "acm:ListTagsForCertificate",
    "acm:GetAccountConfiguration"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSChatbotServiceLinkedRolePolicy

描述：AWS Chatbot 使用的服务关联角色。

AWSChatbotServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 18 日 16:39 UTC
- 编辑时间：2019 年 11 月 18 日 16:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsFullAccess

描述：允许完全访问 AWS 洁净室资源和相关资源 AWS 服务。

AWSCleanRoomsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCleanRoomsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:10 UTC
- 编辑时间：世界标准时间 2024 年 3 月 21 日 15:35
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsFullAccessNoQuerying

描述：允许对 C AWS lean Rooms 资源的完全访问权限，但协作中的查询和相关资源的访问权限除外 AWS 服务。

AWSCleanRoomsFullAccessNoQuerying 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCleanRoomsFullAccessNoQuerying 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:12 UTC
- 编辑时间：世界标准时间 2024 年 5 月 14 日 18:31
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsMLFullAccess

描述：允许对 C AWS lean Rooms 机器学习资源的完全访问权限和对相关资源的访问权限 AWS 服务。

AWSCleanRoomsMLFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCleanRoomsMLFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 21:02
- 编辑时间：世界标准时间 2023 年 11 月 29 日 21:02
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsMLReadOnlyAccess

描述：允许对 C AWS lean Rooms ML 资源进行只读访问以及对相关 AWS 洁净室资源的只读访问权限

AWSCleanRoomsMLReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCleanRoomsMLReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 20:55
- 编辑时间：世界标准时间 2023 年 11 月 29 日 20:55
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsReadOnlyAccess

描述：允许对 C AWS lean Rooms 资源进行只读访问以及对相关 AWS Glue 和 Amazon CloudWatch Logs 资源的只读访问权限。

AWSCleanRoomsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSCleanRoomsReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:10 UTC
- 编辑时间：2023 年 1 月 12 日 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWS Cloud9Administrator

描述：提供对 AWS Cloud9 的管理员访问权限。

AWS Cloud9Administrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloud9Administrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:17 UTC
- 编辑时间：2023 年 10 月 11 日 12:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9Administrator

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloud9EnvironmentMember

描述：提供受邀加入 AWS Cloud9 共享开发环境的功能。

AWSCloud9EnvironmentMember 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloud9EnvironmentMember 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:18 UTC
- 编辑时间：2023 年 10 月 11 日 12:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloud9ServiceRolePolicy

描述：AWS Cloud9 的服务关联角色策略

AWSCloud9ServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 30 日 13:44 UTC
- 编辑时间：2022 年 1 月 17 日 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloud9SSMInstanceProfile

描述：此策略将用于在上附加一个角色， InstanceProfile 该角色将允许 Cloud9 使用 SSM 会话管理器连接到实例

AWSCloud9SSMInstanceProfile是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCloud9SSMInstanceProfile 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 14 日 11:40 UTC
- 编辑时间：2020 年 5 月 14 日 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloud9User

描述：提供创建 AWS Cloud9 开发环境和管理自有环境的权限。

AWSCloud9User 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloud9User 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2017 年 11 月 30 日 16:16 UTC
- 编辑时间：2023 年 10 月 11 日 13:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudFormationFullAccess

描述：提供对的完全访问权限 AWS CloudFormation。

AWSCloudFormationFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudFormationFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 26 日 21:50 UTC
- 编辑时间：2019 年 7 月 26 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudFormationReadOnlyAccess

描述：AWS CloudFormation 通过提供访问权限 AWS Management Console。

AWSCloudFormationReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudFormationReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2019 年 11 月 13 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudFrontLogger

描述：授予 CloudFront Logger 对 CloudWatch 日志的写入权限。

AWSCloudFrontLogger 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 12 日 20:15 UTC
- 编辑时间：2019 年 11 月 22 日 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudHSMFullAccess

描述：提供对所有 CloudHSM 资源的完全访问权限。

AWSCloudHSMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudHSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudHSMReadOnlyAccess

描述：提供对所有 CloudHSM 资源的只读访问权限。

AWSCloudHSMReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudHSMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudHSMRole

描述 : AWS CloudHSM 服务角色的默认策略。

AWSCloudHSMRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudHSMRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```



```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudMapDiscoverInstanceAccess

描述：提供对 AWS Cloud 地图发现 API 的访问权限。

AWSCloudMapDiscoverInstanceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudMapDiscoverInstanceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 00:02 UTC
- 编辑时间：2023 年 9 月 20 日 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudMapFullAccess

描述：提供对所有 AWS Cloud 地图操作的完全访问权限。

AWSCloudMapFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudMapFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 23:57 UTC
- 编辑时间：2020 年 7 月 29 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudMapReadOnlyAccess

描述：提供对所有 AWS Cloud 地图操作的只读访问权限。

AWSCloudMapReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudMapReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 23:45 UTC
- 编辑时间：2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudMapRegisterInstanceAccess

描述：为注册人提供对 AWS Cloud 地图操作的访问权限。

AWSCloudMapRegisterInstanceAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudMapRegisterInstanceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 00:04 UTC
- 编辑时间：2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWS CloudShellFullAccess

说明：使用所有功能 AWS CloudShell 即可获得奖励

AWSCloudShellFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudShellFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:07 UTC
- 编辑时间：2020 年 12 月 15 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudTrail_FullAccess

描述：提供对的完全访问权限 AWS CloudTrail。

AWSCloudTrail_FullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudTrail_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 8 日 23:41 UTC
- 编辑时间：2021 年 2 月 22 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudTrail_ReadOnlyAccess

描述：提供对的只读访问权限 AWS CloudTrail。

AWSCloudTrail_ReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCloudTrail_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 6 月 14 日 17:19 UTC
- 编辑时间：2022 年 6 月 14 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

描述：此策略由名为 `AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents` 的服务相关角色使用。CloudWatch 当 CloudWatch 警报进入警报状态时，使用此服务相关角色执行 AWS 系统管理员事件管理器操作。此策略授予代表您启动事件的权限。

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 27 日 13:30 UTC
- 编辑时间：2021 年 4 月 27 日 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeArtifactAdminAccess

描述：AWS CodeArtifact 通过提供对的完全访问权限 AWS Management Console。

AWSCodeArtifactAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeArtifactAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 16 日 23:53 UTC
- 编辑时间：2020 年 6 月 16 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeArtifactReadOnlyAccess

描述：AWS CodeArtifact 通过提供只读访问权限 AWS Management Console。

AWSCodeArtifactReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeArtifactReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 25 日 21:23 UTC
- 编辑时间：2020 年 6 月 25 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeBuildAdminAccess

描述：AWS CodeBuild 通过提供对的完全访问权限 AWS Management Console。还ReadOnlyAccess 要附加 AmazonS3 以提供下载构建项目的访问权限，并附加 IAM FullAccess 以创建和管理其服务角色。CodeBuild

AWSCodeBuildAdminAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSCodeBuildAdminAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 19:04 UTC
- 编辑时间：世界标准时间 2024 年 5 月 2 日 01:45
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "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" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeBuildDeveloperAccess

描述：AWS CodeBuild 通过提供访问权限 AWS Management Console，但不允许 CodeBuild 项目管理。还要附上 AmazonS3 ReadOnlyAccess 以提供下载构建项目的访问权限。

AWSCodeBuildDeveloperAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeBuildDeveloperAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 19:02 UTC
- 编辑时间：世界标准时间 2024 年 5 月 2 日 01:36
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeBuildReadOnlyAccess

描述：AWS CodeBuild 通过提供只读访问权限 AWS Management Console。还要附上 AmazonS3 ReadOnlyAccess 以提供下载构建项目的访问权限。

AWSCodeBuildReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeBuildReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 19:03 UTC
- 编辑时间：世界标准时间 2024 年 5 月 2 日 01:23
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

策略版本

策略版本：v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets"
  ],
  "Resource" : "*"
}
],
"Version" : "2012-10-17"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeCommitFullAccess

描述：AWS CodeCommit 通过提供对的完全访问权限 AWS Management Console。

AWSCodeCommitFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeCommitFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:02 UTC
- 编辑时间：2023 年 7 月 17 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "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/*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeCommitPowerUser

描述：提供对 AWS CodeCommit 存储库的完全访问权限，但不允许删除存储库。

AWSCodeCommitPowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeCommitPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:06 UTC
- 编辑时间：2023 年 7 月 17 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeCommitReadOnly

描述：AWS CodeCommit 通过提供只读访问权限 AWS Management Console。

AWSCodeCommitReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeCommitReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:05 UTC

- 编辑时间：2021 年 8 月 18 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
  "StringLike" : {
    "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployDeployerAccess

描述：提供注册和部署修订版的权限。

AWSCodeDeployDeployerAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployDeployerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 19 日 18:18 UTC
- 编辑时间：2020 年 4 月 2 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
    }
  }
},
{
  "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" : "*"
}
```

```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployFullAccess

描述：提供对 CodeDeploy 资源的完全访问权限。

AWSCodeDeployFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 19 日 18:13 UTC
- 编辑时间：2020 年 4 月 2 日 16:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
      "StringLike" : {
        "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
      }
    }
  },
  {
    "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployReadOnlyAccess

描述：提供对 CodeDeploy 资源的只读访问权限。

AWSCodeDeployReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 5 月 19 日 18:21 UTC
- 编辑时间：2020 年 4 月 2 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
```

```
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListEventTypes",
      "codestar-notifications:ListTargets"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRole

描述：提供 CodeDeploy 服务访问权限，以扩展标签并代表您与 Auto Scaling 进行交互。

AWSCodeDeployRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 4 日 18:05 UTC
- 编辑时间：2023 年 8 月 16 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRoleForCloudFormation

描述：提供 CodeDeploy 服务访问权限，以代表您调用 Lambda 函数以通过执行蓝/绿部署。
CloudFormation

AWSCodeDeployRoleForCloudFormation 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployRoleForCloudFormation 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 5 月 19 日 17:12 UTC
- 编辑时间：2020 年 5 月 19 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRoleForECS

描述：提供 CodeDeploy 服务范围的访问权限，以代表您执行 ECS 蓝/绿部署。授予对支持服务的完全访问权限，例如读取所有 S3 对象、调用所有 Lambda 函数、发布到账户内的所有 SNS 主题以及更新所有 ECS 服务的完全访问权限。

AWSCodeDeployRoleForECS是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSCodeDeployRoleForECS` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 20:40 UTC
- 编辑时间：2019 年 9 月 23 日 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRoleForECSLimited

描述：提供 CodeDeploy 服务有限访问权限，以代表您执行 ECS 蓝/绿部署。

AWSCodeDeployRoleForECSLimited 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployRoleForECSLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2018 年 11 月 27 日 20:42 UTC
- 编辑时间 : 2019 年 9 月 23 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRoleForLambda

描述：提供 CodeDeploy 服务访问权限以代表您执行 Lambda 部署。

AWSCodeDeployRoleForLambda 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployRoleForLambda 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 28 日 14:05 UTC
- 编辑时间：2019 年 12 月 3 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeDeployRoleForLambdaLimited

描述：提供 CodeDeploy 服务受限访问权限以代表您执行 Lambda 部署。

AWSCodeDeployRoleForLambdaLimited 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeDeployRoleForLambdaLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 17 日 17:14 UTC
- 编辑时间：2020 年 8 月 17 日 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodePipeline_FullAccess

描述：AWS CodePipeline 通过提供对的完全访问权限 AWS Management Console。

AWSCodePipeline_FullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCodePipeline_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 3 日 22:38 UTC
- 编辑时间：世界标准时间 2024 年 3 月 14 日 17:06
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodePipeline_ReadOnlyAccess

描述：AWS CodePipeline 通过提供只读访问权限 AWS Management Console。

AWSCodePipeline_ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodePipeline_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 3 日 22:25 UTC

- 编辑时间：2020 年 8 月 3 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodePipelineApproverAccess

描述：提供查看和批准所有管道的手动更改的权限

AWSCodePipelineApproverAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCodePipelineApproverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 7 月 28 日 18:59 UTC
- 编辑时间：2017 年 8 月 2 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodePipelineCustomActionAccess

描述：为自定义操作提供访问权限，以轮询作业详细信息（包括临时证书）并向其报告状态更新 AWS CodePipeline。

AWSCodePipelineCustomActionAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSCodePipelineCustomActionAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:02 UTC
- 编辑时间：2015 年 7 月 9 日 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeStarFullAccess

描述：AWS CodeStar 通过提供对的完全访问权限 AWS Management Console。

AWSCodeStarFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeStarFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 19 日 16:23 UTC
- 编辑时间：2023 年 3 月 28 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeStarNotificationsServiceRolePolicy

描述：允许 AWS CodeStar 通知代表您访问亚马逊 CloudWatch 活动

AWSCodeStarNotificationsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 5 日 16:10 UTC
- 编辑时间：2020 年 3 月 19 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodeStarServiceRole

描述：请勿使用- AWS CodeStar 服务角色策略，该策略授予管理权限，以便代表客户管理 IAM 和其他服务资源。 CodeStar

AWSCodeStarServiceRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSCodeStarServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 4 月 19 日 15:20 UTC
- 编辑时间：2021 年 9 月 20 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

```
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCompromisedKeyQuarantine

描述：拒绝访问某些操作，这些操作由 AWS 团队在 IAM 用户的证书遭到泄露或公开泄露时应用。请勿删除此策略。相反，您应该会收到有关此事件的电子邮件，请按照其中指定的说明进行操作。

AWSCompromisedKeyQuarantine 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCompromisedKeyQuarantine 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 11 日 18:04 UTC
- 编辑时间：2020 年 8 月 11 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCompromisedKeyQuarantineV2

描述：拒绝访问某些操作，这些操作由 AWS 团队在 IAM 用户的证书遭到泄露或公开泄露时应用。请勿删除此策略。相反，请按照为您创建的此事件相关支持案例中指定的说明进行操作。

AWSCompromisedKeyQuarantineV2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCompromisedKeyQuarantineV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 21 日 22:30 UTC
- 编辑时间：2023 年 3 月 16 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigMultiAccountSetupPolicy

描述：允许 Config 调用 AWS 服务并在整个组织中部署配置资源

AWSConfigMultiAccountSetupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 17 日 18:03 UTC
- 编辑时间：2023 年 2 月 24 日 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigRemediationServiceRolePolicy

描述：允许 AWS Config 代表您修复不合规的资源。

AWSConfigRemediationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 18 日 21:21 UTC
- 编辑时间：2019 年 6 月 18 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigRoleForOrganizations

描述：允许 AWS Config 调用只读 AWS Organizations

AWSConfigRoleForOrganizations 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSConfigRoleForOrganizations 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 3 月 19 日 22:53 UTC
- 编辑时间：2020 年 11 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigRulesExecutionRole

描述：允许 AWS Lambda 函数访问配置 API 和 AWS 配置快照，这些快照由 Config 定期发送到 Amazon S3。对自定义 Config 规则的配置更改执行评估的函数需要此访问权限。

AWSConfigRulesExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSConfigRulesExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 3 月 25 日 17:59 UTC
- 编辑时间：2019 年 5 月 13 日 21:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigServiceRolePolicy

描述：允许 Config 代表您调用 AWS 服务并收集资源配置。

AWSConfigServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 30 日 23:31 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 17:20
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy

策略版本

策略版本：v50 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"app-integrations:GetEventIntegration",
"app-integrations:ListEventIntegrationAssociations",
"app-integrations:ListEventIntegrations",
"appconfig:GetApplication",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetExtensionAssociation",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"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: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",
"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:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch: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",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
```

```
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"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",
"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",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config:Select*",
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
```

```
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
"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",
"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",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"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:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"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",
"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:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
```

```
"emr-serverless:ListApplications",
"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:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTags",
"glue:GetWorkflow",
"glue:ListCrawlers",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"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",
"imagebuilder:GetComponent",
"imagebuilder:GetContainerRecipe",
"imagebuilder:GetDistributionConfiguration",
"imagebuilder:GetImage",
"imagebuilder:GetImagePipeline",
"imagebuilder:GetImageRecipe",
"imagebuilder:GetInfrastructureConfiguration",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
```

```
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"inspector2:BatchGetAccountStatus",
"inspector2:GetDelegatedAdminAccount",
"inspector2:ListFilters",
"inspector2:ListMembers",
"iot:DescribeAccountAuditConfiguration",
"iot:DescribeAuthorizer",
"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:GetPolicy",
"iot:GetTopicRule",
"iot:GetTopicRuleDestination",
"iot:ListAuthorizers",
"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: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",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"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:GetFuotaTask",
```

```
"iotwireless:GetMulticastGroup",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:GetChannel",
"ivs:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamKey",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreamKeys",
"ivs: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:GetFunction",
"lambda:GetFunctionCodeSigningConfig",
"lambda:GetLayerVersion",
"lambda:GetPolicy",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"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:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:GetDataProtectionPolicy",
"logs:GetLogDelivery",
"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:ListCustomDataIdentifiers",
```

```
"macie2:ListTagsForResource",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNodes",
"mediaconnect:DescribeFlow",
"mediaconnect:ListFlows",
"mediaconnect:ListTagsForResource",
"mediapackage-vod:DescribePackagingConfiguration",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mediapackage-vod:ListTagsForResource",
"mediatailor:GetPlaybackConfiguration",
"mediatailor:ListPlaybackConfigurations",
"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:GetTransitGatewayRegistrations",
"networkmanager:ListConnectPeers",
"networkmanager:ListTagsForResource",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetStreamingImage",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStudioComponents",
"nimble:ListStudios",
"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",
```

```
"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",
"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:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshotAttributes",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"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:DescribeLoggingStatus",
"redshift:DescribeScheduledActions",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListServices",
"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",
"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: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:ListAccessPoints",
"s3:ListAccessPointsForObjectLambda",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"s3:ListStorageLensConfigurations",
"s3express:GetBucketPolicy",
"s3express:ListAllMyDirectoryBuckets",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeFeatureGroup",
```

```
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceExperiment",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribeProject",
"sagemaker:DescribeWorkteam",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListCodeRepositories",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDomains",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListFeatureGroups",
"sagemaker:ListImages",
"sagemaker:ListImageVersions",
"sagemaker:ListInferenceExperiments",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelines",
"sagemaker:ListProjects",
"sagemaker:ListTags",
"sagemaker:ListWorkteams",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"sdb:GetAttributes",
"sdb:ListDomains",
```

```
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:DescribeHub",
"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:GetEmailTemplate",
"ses:GetTemplate",
"ses:ListConfigurationSets",
"ses:ListContactLists",
"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:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:DescribeDocumentPermission",
```

```
"ssm:DescribeParameters",
"ssm:GetAutomationExecution",
"ssm:GetDocument",
"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",
    "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:*::/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/*"
]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigUserAccess

描述：提供使用 AWS Config 的权限，包括按资源上的标签搜索和读取所有标签。这不提供配置 AWS Config 的权限，这需要管理员权限。

AWSConfigUserAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSConfigUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 18 日 19:38 UTC
- 编辑时间：2019 年 3 月 18 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConnector

描述：启用对所有 EC2 对象的广泛读/写访问权限、对以“import-to-ec2-”开头的 S3 存储桶的读/写访问权限，并能够列出所有 S3 存储桶，以便连接器代表您导入虚拟机。AWS

AWSConnector 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSConnector 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 11 日 17:14 UTC
- 编辑时间：2015 年 9 月 28 日 19:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:DescribeInstanceState",
    "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-*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSControlTowerAccountServiceRolePolicy

描述：允许 Cont AWS rol Tower 代表您调用提供自动账户配置和集中管理的 AWS 服务。

AWSControlTowerAccountServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 5 日 22:04 UTC
- 编辑时间：2023 年 6 月 5 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSControlTowerServiceRolePolicy

描述：提供对 Control Tower AWS 管理或使用的 AWS 资源的访问权限

AWSControlTowerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSControlTowerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 5 月 3 日 18:19 UTC

- 编辑时间 : 2023 年 4 月 12 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

策略版本

策略版本 : v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCostAndUsageReportAutomationPolicy

描述：授予权限以描述账户的组织、为 MAP 程序创建 S3 存储桶并对其应用标签、创建成本和使用情况报告以及描述成本和使用情况报告定义。

AWSCostAndUsageReportAutomationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSCostAndUsageReportAutomationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 1 日 21:27 UTC
- 编辑时间：2021 年 11 月 1 日 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataExchangeFullAccess

描述：使用和 SDK 授予对 D AWS ata Exchange AWS Management Console 和 AWS Marketplace 操作的完全访问权限。它还提供对充分利用 D AWS ata Exchange 所需的相关服务的精选访问权限。

AWSDataExchangeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDataExchangeFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 19:27 UTC
- 编辑时间：世界标准时间 2024 年 5 月 7 日 17:04
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetPrivateListing",
      "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataExchangeProviderFullAccess

描述：使用和 SDK 向 AWS 数据提供者授予对 Data Exchange AWS Management Console 和 AWS Marketplace 操作的访问权限。它还提供对充分利用 D AWS ata Exchange 所需的相关服务的精选访问权限。

AWSDataExchangeProviderFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataExchangeProviderFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 19:27 UTC
- 编辑时间：2022 年 3 月 15 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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",
    "tag:GetTagKeys",
    "tag:GetTagValues"
  ],
  "Resource" : "*"
},
{
  "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"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "arn:aws:s3::*aws-data-exchange*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {

```

```
        "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
        ]
    }
}
},
{
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
        "StringEqualsIgnoreCase" : {
            "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "dataexchange.amazonaws.com"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
    ],
    "Resource" : "arn:aws:s3::*aws-data-exchange*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "dataexchange.amazonaws.com"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
}
```

```
  },
  {
    "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" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
      "kms:ListKeys"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "redshift:AuthorizeDataShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "redshift:ConsumerIdentifier" : "ADX"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataExchangeReadOnly

描述：使用和 SDK 授予对 D AWS ata Exchange AWS Management Console 和 AWS Marketplace 操作的只读访问权限。

AWSDataExchangeReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDataExchangeReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 19:27 UTC
- 编辑时间：2021 年 5 月 10 日 21:15 UTC

- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataExchangeSubscriberFullAccess

描述：使用 SDK 向 AWS 数据订阅者授予对 Data Exchange AWS Management Console 和 AWS Marketplace 操作的访问权限。它还提供对充分利用 Data Exchange 所需的相关服务的精选访问权限。

AWSDataExchangeSubscriberFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataExchangeSubscriberFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 19:27 UTC
- 编辑时间：世界标准时间 2024 年 5 月 21 日 17:36
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataLifecycleManagerServiceRole

描述：为 AWS 数据生命周期管理员提供对 AWS 资源采取操作的相应权限

AWSDataLifecycleManagerServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataLifecycleManagerServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 7 月 6 日 19:34 UTC
- 编辑时间：2022 年 9 月 19 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
    ],
    "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.*"
  }
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

描述：为 AWS 数据生命周期管理员提供相应权限，允许他们对 AMI 管理的 AWS 资源采取操作

AWSDataLifecycleManagerServiceRoleForAMIManagement 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataLifecycleManagerServiceRoleForAMIManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 10 月 21 日 19:39 UTC
- 编辑时间：2021 年 8 月 19 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AWSDataLifecycleManagerServiceRoleForAMIManagement

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataLifecycleManagerSSMFullAccess

描述：提供 Amazon Data Lifecycle Manager 权限，允许其执行在所有 Amazon EC2 实例上运行预脚本和后置脚本所需的系统管理器操作。

AWSDataLifecycleManagerSSMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataLifecycleManagerSSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 10 月 31 日 20:29 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 22:31
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataPipeline_FullAccess

描述：提供对 Data Pipeline 的完全访问权限、S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的列表访问权限以及默认角色的 PassRole 访问权限。

AWSDataPipeline_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataPipeline_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 19 日 23:14 UTC

- 编辑时间：2017 年 8 月 17 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataPipeline_PowerUser

描述：提供对 Data Pipeline 的完全访问权限、S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的列表访问权限以及默认角色的 PassRole 访问权限。

AWSDataPipeline_PowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDataPipeline_PowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 19 日 23:16 UTC
- 编辑时间：2017 年 8 月 17 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataSyncDiscoveryServiceRolePolicy

描述：允许 DataSync Discovery 代表您与其他 AWS 服务集成。

AWSDataSyncDiscoveryServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 20 日 22:19 UTC
- 编辑时间：2023 年 3 月 20 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataSyncFullAccess

描述：提供对其依赖项的完全访问权限 AWS DataSync 和最低限度访问权限

AWSDataSyncFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDataSyncFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 19:40 UTC
- 编辑时间：世界标准时间 2024 年 2 月 16 日 17:19
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "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"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DataSyncPassRolePermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "datasync.amazonaws.com"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataSyncReadOnlyAccess

描述：提供对的只读访问权限 AWS DataSync

AWSDataSyncReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDataSyncReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 19:18 UTC
- 编辑时间：2020 年 6 月 30 日 17:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-FleetWorker

描述：为 De AWS adline Cloud 工作人员提供在服务器场上运行任务的访问权限。

AWSDeadlineCloud-FleetWorker是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-FleetWorker 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 17:21
- 编辑时间：世界标准时间 2024 年 4 月 1 日 17:21
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-UserAccessFarms

描述：使用有限的只读权限为用户提供对 De AWS adline Cloud 场的工作站访问权限，以调用其他必要服务。将此策略附加到与您的工作室关联的用户角色。

AWSDeadlineCloud-UserAccessFarms是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-UserAccessFarms 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 16:54
- 编辑时间：世界标准时间 2024 年 4 月 1 日 16:54
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetQueue",
    "deadline:GetQueueEnvironment",
    "deadline:GetQueueFleetAssociation",
    "deadline:GetSession",
    "deadline:GetSessionAction",
    "deadline:GetStep",
    "deadline:GetStorageProfile",
    "deadline:GetStorageProfileForQueue",
    "deadline:GetTask",
    "deadline:GetWorker",
    "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}"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-UserAccessFleets

描述：允许用户在工作站访问 De AWS adline Cloud 舰队，并具有有限的只读权限，可以调用其他必要服务。将此策略附加到与您的工作室关联的用户角色。

AWSDeadlineCloud-UserAccessFleets 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-UserAccessFleets 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 17:01
- 编辑时间：世界标准时间 2024 年 4 月 1 日 17:01
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-UserAccessJobs

描述：允许用户在工作站访问 Deadlin AWS e Cloud 作业，但只读权限有限，可以调用其他必要服务。将此策略附加到与您的工作室关联的用户角色。

AWSDeadlineCloud-UserAccessJobs是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-UserAccessJobs 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 17:05
- 编辑时间：世界标准时间 2024 年 4 月 1 日 17:05
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "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}"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-UserAccessQueues

描述：使用有限的只读权限为用户提供对De AWS adline Cloud队列的访问权限，以调用其他必要服务。将此策略附加到与您的工作室关联的用户角色。

AWSDeadlineCloud-UserAccessQueues是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-UserAccessQueues 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 17:10
- 编辑时间：世界标准时间 2024 年 4 月 1 日 17:10
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:GetQueue",
    "deadline:GetQueueEnvironment",
    "deadline:GetQueueFleetAssociation",
    "deadline:GetSession",
    "deadline:GetSessionAction",
    "deadline:GetStep",
    "deadline:GetStorageProfileForQueue",
    "deadline:GetTask",
    "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}"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeadlineCloud-WorkerHost

描述：为 Deadlin AWS e Cloud 工作人员主机提供加入场中队列的访问权限。

AWSDeadlineCloud-WorkerHost是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeadlineCloud-WorkerHost 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 4 月 1 日 17:28
- 编辑时间：世界标准时间 2024 年 4 月 1 日 17:28
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepLensLambdaFunctionAccessPolicy

描述：此策略指定在设备上运行的 DeepLens 管理 lambda 函数所需的权限 DeepLens

AWSDeepLensLambdaFunctionAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeepLensLambdaFunctionAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 15:47 UTC
- 编辑时间：2019 年 6 月 11 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepLensServiceRolePolicy

描述：授予 AWS DeepLens 访问权限及其依赖项（包括 IoT AWS 服务、S3 DeepLens 和 AWS Lambda）所需的资源 GreenGrass 和角色。

AWSDeepLensServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeepLensServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 29 日 15:46 UTC
- 编辑时间：2019 年 9 月 25 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

策略版本

策略版本：v6（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerAccountAdminAccess

描述：DeepRacer 管理员可以访问所有操作，包括在多用户模式和单用户模式之间切换。

AWSDeepRacerAccountAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDeepRacerAccountAdminAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 28 日 01:27 UTC
- 编辑时间：2021 年 10 月 28 日 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerCloudFormationAccessPolicy

描述：CloudFormation 允许代表您创建和管理 AWS 堆栈和资源。

AWSDeepRacerCloudFormationAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeepRacerCloudFormationAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 2 月 28 日 21:59 UTC
- 编辑时间：2019 年 6 月 14 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerDefaultMultiUserAccess

描述：在多用户 DeepRacer MultiUser 模式下使用 deepracer 的默认用户访问权限

AWSDeepRacerDefaultMultiUserAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDeepRacerDefaultMultiUserAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 28 日 01:27 UTC
- 编辑时间：2021 年 10 月 28 日 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerFullAccess

描述：提供对的完全访问权限 AWS DeepRacer。还提供对相关服务（例如 S3）的部分访问权限。

AWSDeepRacerFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDeepRacerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 5 日 22:03 UTC
- 编辑时间：2020 年 10 月 5 日 22:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerRoboMakerAccessPolicy

描述：RoboMaker 允许创建所需资源并代表您呼叫 AWS 服务。

AWSDeepRacerRoboMakerAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDeepRacerRoboMakerAccessPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 2 月 28 日 21:59 UTC
- 编辑时间：2019 年 2 月 28 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeepRacerServiceRolePolicy

描述：DeepRacer 允许创建所需资源并代表您呼叫 AWS 服务。

AWSDeepRacerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeepRacerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 2 月 28 日 21:58 UTC
- 编辑时间：2019 年 6 月 12 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDenyAll

描述：拒绝所有访问权限。

AWSDenyAll 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDenyAll 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 1 日 22:36 UTC
- 编辑时间：世界标准时间 2023 年 12 月 18 日 16:42
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeviceFarmFullAccess

描述：提供对 Dev AWS ice Farm 所有操作的完全访问权限。

AWSDeviceFarmFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDeviceFarmFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 7 月 13 日 16:37 UTC
- 编辑时间：2015 年 7 月 13 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeviceFarmServiceRolePolicy

描述：向 Dev AWS ice Farm 授予代表您调用 EC2 网络 API 的权限。

AWSDeviceFarmServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 20 日 21:02 UTC
- 编辑时间：2022 年 9 月 20 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDeviceFarmTestGridServiceRolePolicy

描述：向 Dev AWS ice Farm 授予代表您调用 EC2 API 的权限。

AWSDeviceFarmTestGridServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 26 日 22:01 UTC
- 编辑时间：2021 年 5 月 26 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDirectConnectFullAccess

描述：提供通过 Di AWS rect Connect 的完全访问权限 AWS Management Console。

AWSDirectConnectFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDirectConnectFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 4 月 30 日 15:29 UTC

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

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDirectConnectReadOnlyAccess

描述 : 通过提供对 Di AWS rect Connect 的只读访问权限 AWS Management Console。

AWSDirectConnectReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSDirectConnectReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 5 月 18 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDirectConnectServiceRolePolicy

描述：提供代表您创建和管理 AWS 资源的 Di AWS rect Connect 权限。

AWSDirectConnectServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 1 月 14 日 18:35 UTC
- 编辑时间：2021 年 1 月 14 日 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:*directconnect*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDirectoryServiceFullAccess

描述：提供对 Di AWS rectory Service 的完全访问权限。

AWSDirectoryServiceFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSDirectoryServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 4 月 2 日 20:38
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDirectoryServiceReadOnlyAccess

描述：提供对 AWS Directory Service 的只读访问权限。

AWSDirectoryServiceReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDirectoryServiceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2018 年 9 月 25 日 21:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDiscoveryContinuousExportFirehosePolicy

描述：提供对 AWS Discovery 持续导出所需 AWS 资源的写入权限

AWSDiscoveryContinuousExportFirehosePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSDiscoveryContinuousExportFirehosePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 8 月 9 日 18:29 UTC
- 编辑时间：2021 年 6 月 8 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDMSFleetAdvisorServiceRolePolicy

描述：允许 DMS Fleet Advisor 代表您管理 CloudWatch 指标。

AWSDMSFleetAdvisorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 6 日 09:10 UTC
- 编辑时间：2023 年 3 月 6 日 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDMSServerlessServiceRolePolicy

描述：授予 AWS DMS Serverless 权限以代表您创建和管理账户中的 DMS 资源

AWSDMSServerlessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 5 月 18 日 20:28 UTC
- 编辑时间：2023 年 5 月 18 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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>DeleteReplicationTask",
        "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:*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEC2CapacityReservationFleetRolePolicy

描述：允许 EC2 CapacityReservation 队列服务管理容量预留

AWSEC2CapacityReservationFleetRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 29 日 14:43 UTC
- 编辑时间：2021 年 9 月 29 日 14:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
        "StringLike" : {
```

```
        "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"
        }
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEC2FleetServiceRolePolicy

描述：允许 EC2 队列启动和管理实例。

AWSEC2FleetServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 21 日 00:08 UTC

- 编辑时间：2020 年 5 月 4 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
        }
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEC2SpotFleetServiceRolePolicy

描述：允许 EC2 竞价型队列启动和管理竞价型队列实例

AWSEC2SpotFleetServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 23 日 19:13 UTC
- 编辑时间：2020 年 3 月 16 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*/*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEC2SpotServiceRolePolicy

描述：允许 EC2 Spot 启动和管理竞价型实例

AWSEC2SpotServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 18 日 18:51 UTC
- 编辑时间：2018 年 12 月 12 日 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEC2VssSnapshotPolicy

描述：此策略附加到您的 Amazon EC2 Windows 实例的 IAM 角色，允许亚马逊 EC2 VSS 解决方案为亚马逊系统映像 (AMI) 和 EBS 快照创建和添加标签。

AWSEC2VssSnapshotPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSEC2VssSnapshotPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 3 月 27 日 16:32
- 编辑时间：世界标准时间 2024 年 3 月 27 日 16:32
- ARN: arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "DescribeInstanceInfo",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceAttribute"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
      }
    }
  },
  {
    "Sid" : "CreateSnapshotsWithTag",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshots"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AwsVssConfig" : "*"
      }
    }
  },
  {
    "Sid" : "CreateSnapshotsAccessInstance",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshots"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:SourceInstanceARN" : "*${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" : {
    "StringLike" : {
      "ec2:SourceInstanceARN" : "*${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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSECRPullThroughCache_ServiceRolePolicy

描述：允许访问 AWS ECR 通过缓存提取使用或管理的 AWS 服务和资源

AWSECRPullThroughCache_ServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 26 日 21:51 UTC
- 编辑时间：2023 年 11 月 13 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

描述：在您的自定义平台构建器环境中为实例提供启动 EC2 实例、创建 EBS 快照和 AMI、将日志流式传输到 Amazon Logs 以及在 Amazon CloudWatch S3 中存储工件的权限。

AWSElasticBeanstalkCustomPlatformforEC2Role 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkCustomPlatformforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 21 日 22:50 UTC
- 编辑时间：2017 年 2 月 21 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkEnhancedHealth

描述：健康监控系统的 E AWS lastic Beanstalk 服务策略

AWSElasticBeanstalkEnhancedHealth是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkEnhancedHealth 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 8 日 23:17 UTC
- 编辑时间：2018 年 4 月 9 日 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkMaintenance

描述：Elastic Beanstalk 服务角色策略，该策略授予有限的权限，允许您出于维护目的代表您更新资源。

AWSElasticBeanstalkMaintenance 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 1 月 11 日 23:22 UTC
- 编辑时间：世界标准时间 2024 年 4 月 29 日 21:48
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

描述：此策略适用于用于对 E AWS lastic Beanstalk 环境执行托管更新的弹性 Beanstalk 服务角色。不应将此策略附加到其他用户或角色。该策略授予了在许多 AWS 服务中创建和管理资源的广泛权限，包

括 EC2 AutoScaling、ECS、Elastic Load Balancing 和 CloudFormation。该策略还允许传递可与这些服务一起使用的任何 IAM 角色。

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 3 日 22:18 UTC
- 编辑时间：2023 年 3 月 23 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

描述：Elastic Beanstalk 服务角色策略，用于授予对托管更新的有限权限。

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 21 日 22:35 UTC
- 编辑时间：世界标准时间 2024 年 4 月 29 日 23:11
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkMulticontainerDocker

描述：为您的多容器 Docker 环境中的实例提供使用亚马逊 EC2 容器服务管理容器部署任务的访问权限。

AWSElasticBeanstalkMulticontainerDocker 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkMulticontainerDocker 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:15 UTC
- 编辑时间：2023 年 3 月 23 日 22:04 UTC

- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkReadOnly

描述：授予只读权限。明确允许操作员获得直接访问权限，以检索与 E AWS lastic Beanstalk 应用程序相关的资源信息。

AWSElasticBeanstalkReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 19:02 UTC
- 编辑时间：2021 年 1 月 22 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleCore

描述：AWSElasticBeanstalkRoleCore（Elastic Beanstalk 操作角色）允许 Web 服务环境的核心操作。

AWSElasticBeanstalkRoleCore 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleCore 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:48 UTC
- 编辑时间：世界标准时间 2024 年 4 月 30 日 00:01
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

策略版本

策略版本：v3（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleCWL

描述：(Elastic Beanstalk 操作角色) 允许环境管理 CloudWatch 亚马逊日志组。

AWSElasticBeanstalkRoleCWL 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleCWL 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:49 UTC
- 编辑时间：2020 年 6 月 5 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
```

```
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleECS

描述：(Elastic Beanstalk 操作角色) 允许多容器 Docker 环境管理亚马逊 ECS 集群。

AWSElasticBeanstalkRoleECS是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleECS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:47 UTC
- 编辑时间：2023 年 3 月 23 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleRDS

描述：(Elastic Beanstalk 操作角色) 允许环境集成 Amazon RDS 实例。

AWSElasticBeanstalkRoleRDS 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleRDS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:46 UTC
- 编辑时间：2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleSNS

描述：(Elastic Beanstalk 操作角色) 允许环境启用亚马逊 SNS 主题集成。

AWSElasticBeanstalkRoleSNS是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleSNS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:46 UTC
- 编辑时间：2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkRoleWorkerTier

描述：(Elastic Beanstalk 操作角色) 允许工作环境层创建亚马逊 DynamoDB 表和亚马逊 SQS 队列。

AWSElasticBeanstalkRoleWorkerTier 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkRoleWorkerTier 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:43 UTC
- 编辑时间：2020 年 6 月 5 日 21:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkService

描述：此策略已进入弃用路径。有关指导，请参阅文档：<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>。AWS Elastic Beanstalk Service 角色策略，它授予代表您创建和管理资源（AutoScaling即：EC2、CloudFormation S3、ELB 等）的权限。

AWSElasticBeanstalkService是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkService 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 4 月 11 日 20:27 UTC

- 编辑时间：2023 年 5 月 10 日 19:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService

策略版本

策略版本：v17（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkServiceRolePolicy

描述：Elastic Beanstalk 服务关联角色策略，该策略授予代表您创建和管理资源（AutoScaling 即 EC2、CloudFormation S3、ELB 等）的权限。

AWSElasticBeanstalkServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 13 日 23:46 UTC
- 编辑时间：2019 年 6 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkWebTier

描述：向您的 Web 服务器环境中的实例提供将日志文件上传到 Amazon S3 的权限。

AWSElasticBeanstalkWebTier 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkWebTier 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:08 UTC
- 编辑时间：2020 年 9 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticBeanstalkWorkerTier

描述：让您的工作线程环境中的实例能够将日志文件上传到 Amazon S3，使用 Amazon SQS 监控应用程序的任务队列，使用 Amazon DynamoDB 执行领导者选举，以及允许 CloudWatch 亚马逊发布运行状况监控指标。

AWSElasticBeanstalkWorkerTier 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticBeanstalkWorkerTier 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:12 UTC
- 编辑时间：2020 年 9 月 9 日 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

描述：此策略允许安装 AWS 复制代理，该代理与 AWS Elastic 灾难恢复 (DRS) 一起使用，用于将外部服务器恢复到 AWS。将此策略附加到您正在 AWS 复制代理安装步骤中提供证书的 IAM 用户或角色。

AWSElasticDisasterRecoveryAgentInstallationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryAgentInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:37 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 12:38
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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/*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryAgentPolicy

描述：此策略允许使用 AWS 复制代理，该代理与 AWS Elastic 灾难恢复 (DRS) 一起使用，将源服务器恢复到 AWS。我们不建议您将此策略附加到 IAM 用户或角色。

AWSElasticDisasterRecoveryAgentPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryAgentPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:32 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:44
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryConsoleFullAccess

描述：此策略提供对 AWS Elastic 灾难恢复 (DRS) 所有公共 API 的完全访问权限，以及读取 KMS 密钥、许可证管理器、资源组、Elastic Load Balancing、IAM 和 EC2 信息的权限。可将此策略附加到您的 IAM 用户或角色。

AWSElasticDisasterRecoveryConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:46 UTC
- 编辑时间：2023 年 10 月 16 日 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

描述：此策略提供对 AWS Elastic 灾难恢复 (AWS DRS) 的所有公共 API 以及 D AWS RS 控制台使用的其他 AWS 服务中的所有公共 API 的完全访问权限。将此政策附加到您的用户或角色。

AWSElasticDisasterRecoveryConsoleFullAccess_v2是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSElasticDisasterRecoveryConsoleFullAccess_v2` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 27 日 13:35
- 编辑时间：世界标准时间 2024 年 5 月 19 日 07:38
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
    "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/*"
],
"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" : [
      "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"
    ],
    "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"
      }
    }
  }
}
```

```
    }  
  ]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryConversionServerPolicy

描述：此策略附加到 AWS Elastic 灾难恢复转换服务器的实例角色。此策略允许 Elastic Disaster Recovery (DRS) 转换服务器 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务进行通信。DRS 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 DRS 转换服务器 (由 DRS 在需要时自动启动和终止)。我们不建议您将此策略附加到 IAM 用户或角色。当用户选择使用 DRS 控制台、CLI 或 API 恢复源服务器时，Elastic Disaster Recovery 会使用 DRS 转换服务器。

AWSElasticDisasterRecoveryConversionServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryConversionServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 13:42 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:13
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

描述：此策略允许 AWS Elastic 灾难恢复 (DRS) 支持跨账户复制和跨账户故障恢复。

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 5 月 14 日 07:16 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 13:19
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

描述：此策略允许安装和使用 AWS 复制代理，AWS Elastic 灾难恢复 (DRS) 使用该代理来恢复在 EC2 (跨区域或跨可用区) 上运行的源服务器。应将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 EC2 实例。

AWSElasticDisasterRecoveryEc2InstancePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryEc2InstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 5 月 26 日 12:30 UTC

- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:39
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

描述：您可以将 AWSElasticDisasterRecoveryFailbackInstallationPolicy 策略附加到您的 IAM 身份。此策略允许安装 Elastic Disaster Recovery 失效自动恢复客户端，该客户端用于将恢复实例失效自动恢复到原始源基础设施。可将此策略附加到您在运行 Elastic Disaster Recovery 失效自动恢复客户端时提供凭证的 IAM 用户或角色。

AWSElasticDisasterRecoveryFailbackInstallationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryFailbackInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 11:02 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:43
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryFailbackInstallationPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryFailbackPolicy

描述：此策略允许使用 Elastic 灾难恢复故障恢复客户端，该客户端用于将恢复实例故障恢复到原始源基础架构。我们不建议您将此策略附加到 IAM 用户或角色。

AWSElasticDisasterRecoveryFailbackPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryFailbackPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:41 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 12:56
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
  }
]
}

```


了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

描述：此策略允许您使用 Amazon SSM 和其他服务所需的权限在 AWS Elastic 灾难恢复 (AWS DRS) 中运行启动后操作。将此策略附加到您的 IAM 角色或用户。

AWSElasticDisasterRecoveryLaunchActionsPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryLaunchActionsPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 13 日 07:38 UTC
- 编辑时间：世界标准时间 2024 年 5 月 19 日 07:29
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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/*:*"
    ],
    "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/AWSDistro0Tel-*",
  "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/AWSDistro0Tel-*:*",
"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-*:*"
],
"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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

描述：此策略允许 AWS Elastic 灾难恢复 (DRS) 支持网络复制。

AWSElasticDisasterRecoveryNetworkReplicationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryNetworkReplicationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 11 日 12:36 UTC
- 编辑时间：世界标准时间 2024 年 1 月 2 日 13:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryReadOnlyAccess

描述：您可以将 AWSElasticDisasterRecoveryReadOnlyAccess 策略附加到您的 IAM 身份。此策略提供对 Elastic Daser Recovery (DRS) 的所有只读公共 API 的权限，以及其他 AWS 服务的一些只读 API 的权限，这些都是完全只读地使用 DRS 控制台所必需的。可将此策略附加到您的 IAM 用户或角色。

AWSElasticDisasterRecoveryReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:50 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:03
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "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"
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

描述：此策略附加到 Elastic 灾难恢复实例的实例角色上。此策略允许 Elastic Disaster Recovery (DRS) 恢复实例 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务通信，并能够对其原始源基础设施执行失效自动恢复。Elastic Disaster Recovery 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 DRS 恢复实例。我们不建议您将此策略附加到 IAM 用户或角色。

AWSElasticDisasterRecoveryRecoveryInstancePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryRecoveryInstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:20 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:11
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

描述：此策略附加到 Elastic 灾难恢复复制服务器的实例角色。此策略允许 Elastic Disaster Recovery (DRS) 复制服务器 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务进行通信，并在您的 AWS 账户中创建 EBS 快照。Elastic Disaster Recovery 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 DRS 复制服务器 (由 DRS 在需要时自动启动和终止)。作为 DRS 管

理的恢复过程的一部分 AWS，DRS 复制服务器用于促进将数据从外部服务器复制到。我们不建议您将此策略附加到 IAM 用户或角色。

AWSElasticDisasterRecoveryReplicationServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryReplicationServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 13:34 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:28
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryServiceRolePolicy

描述：此策略允许 Elastic 灾难恢复代表您管理 AWS 资源。

AWSElasticDisasterRecoveryServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 17 日 10:56 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 13:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "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/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateLaunchTemplate",
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances"
        ]
      }
    }
  },
  {
    "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" : "*"
  }
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

描述：此策略允许对源服务器和作业等 AWS 弹性灾难恢复 (DRS) 资源进行只读访问。它还允许创建一个转换后的快照并与特定账户共享该 EBS 快照。

AWSElasticDisasterRecoveryStagingAccountPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryStagingAccountPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 5 月 26 日 09:49 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

描述： AWS Elastic 灾难恢复 (DRS) 使用此策略将源服务器恢复到单独的目标账户中并允许故障恢复。我们不建议您将此策略附加到 IAM 用户或角色。

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElasticDisasterRecoveryStagingAccountPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 1 月 5 日 12:11 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:32
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

描述： AWS Elastic Load Balancing 控制平面的服务关联角色策略——经典

AWSElasticLoadBalancingClassicServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型：** 服务相关角色策略
- **创建时间：** 2017 年 9 月 19 日 22:36 UTC
- **编辑时间：** 2019 年 10 月 7 日 23:04 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

策略版本

策略版本： v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElasticLoadBalancingServiceRolePolicy

描述： AWS Elastic Load Balancing 控制平面的服务关联角色策略

AWSElasticLoadBalancingServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 19 日 22:19 UTC

- 编辑时间 : 2021 年 8 月 26 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
```

```
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssignIpv6Addresses",
    "ec2:ReleaseAddress",
    "ec2:UnassignIpv6Addresses",
    "ec2:DescribeVpcPeeringConnections",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:ListLogDeliveries",
    "outposts:GetOutpostInstanceTypes"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaConvertFullAccess

描述：提供 MediaConvert 通过 AWS Management Console 和 SDK 对 AWS Elemental 的完全访问权限。

AWSElementalMediaConvertFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaConvertFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 25 日 19:25 UTC
- 编辑时间：2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaConvertReadOnly

描述：MediaConvert 通过 AWS Management Console 和 SDK 提供对 AWS Elemental 的只读访问权限。

AWSElementalMediaConvertReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaConvertReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 25 日 19:25 UTC
- 编辑时间：2019 年 6 月 10 日 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "mediaconvert:List*",
    "mediaconvert:DescribeEndpoints",
    "s3:ListAllMyBuckets",
    "s3:ListBucket"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaLiveFullAccess

描述：提供对 AWS 元素 MediaLive 资源的完全访问权限

AWSElementalMediaLiveFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaLiveFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 8 日 17:07 UTC
- 编辑时间：2020 年 7 月 8 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaLiveReadOnly

描述：提供对 AWS 元素 MediaLive 资源的只读访问权限

AWSElementalMediaLiveReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaLiveReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 8 日 16:38 UTC
- 编辑时间：2020 年 7 月 8 日 16:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaPackageFullAccess

描述：提供对 AWS 元素 MediaPackage 资源的完全访问权限

AWSElementalMediaPackageFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaPackageFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 29 日 23:39 UTC
- 编辑时间：2017 年 12 月 29 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaPackageReadOnly

描述：提供对 AWS 元素 MediaPackage 资源的只读访问权限

AWSElementalMediaPackageReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaPackageReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 30 日 00:04 UTC
- 编辑时间：2017 年 12 月 30 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaPackageV2FullAccess

描述：提供对 AWS Elemental MediaPackage V2 资源的完全访问权限。

AWSElementalMediaPackageV2FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaPackageV2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 20:29 UTC
- 编辑时间：2023 年 7 月 25 日 20:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaPackageV2ReadOnly

描述：提供对 AWS Elemental MediaPackage V2 资源的只读访问权限。

AWSElementalMediaPackageV2ReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaPackageV2ReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 20:31 UTC
- 编辑时间：2023 年 7 月 25 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaStoreFullAccess

描述：提供对所有 MediaStore API 的完全读写权限

AWSElementalMediaStoreFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaStoreFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 5 日 23:15 UTC
- 编辑时间：2018 年 3 月 5 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Action" : [
      "mediastore:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaStoreReadOnly

描述：为 MediaStore API 提供只读权限

AWSElementalMediaStoreReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaStoreReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 8 日 19:48 UTC
- 编辑时间：2018 年 3 月 8 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaTailorFullAccess

描述：提供对 AWS 元素 MediaTailor 资源的完全访问权限

AWSElementalMediaTailorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaTailorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 23 日 00:04 UTC
- 编辑时间：2021 年 11 月 23 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSElementalMediaTailorReadOnly

描述：提供对 AWS 元素 MediaTailor 资源的只读访问权限

AWSElementalMediaTailorReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSElementalMediaTailorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 23 日 00:05 UTC
- 编辑时间：2021 年 11 月 23 日 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEnhancedClassicNetworkingMangementPolicy

描述：启用增强型经典网络管理功能的策略。

AWSEnhancedClassicNetworkingMangementPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 20 日 17:29 UTC
- 编辑时间：2017 年 9 月 20 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEntityResolutionConsoleFullAccess

描述：提供控制台对 AWS 实体解析和相关服务的完全访问权限。

AWSEntityResolutionConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSEntityResolutionConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 17 日 17:54 UTC
- 编辑时间：2023 年 10 月 16 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSEntityResolutionConsoleReadOnlyAccess

描述：通过提供对 AWS 实体解析的只读访问权限 AWS Management Console。

AWSEntityResolutionConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSEntityResolutionConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 17 日 18:18 UTC
- 编辑时间：2023 年 8 月 17 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorEC2Access

描述：此策略授予故障注入模拟器服务在 EC2 和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorEC2Access 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:39 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 15:08
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorECSAccess

描述：此策略授予故障注入模拟器服务在 ECS 和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorECSAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorECSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:37 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 16:16
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorEKSAccess

描述：此策略授予故障注入模拟器服务在 EKS 和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorEKSAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorEKSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:34 UTC
- 编辑时间：2023 年 11 月 13 日 16:44 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorNetworkAccess

描述：此策略授予故障注入模拟器服务在 EC2 网络和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorNetworkAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorNetworkAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:32 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 16:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorRDSAccess

描述：此策略授予故障注入模拟器服务在 RDS 和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorRDSAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorRDSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:30 UTC
- 编辑时间：2023 年 11 月 13 日 16:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFaultInjectionSimulatorSSMAccess

描述：此策略授予故障注入模拟器服务在 SSM 和其他必需服务中执行 FIS 操作的权限。

AWSFaultInjectionSimulatorSSMAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFaultInjectionSimulatorSSMAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2022 年 10 月 26 日 15:33 UTC
- 编辑时间：2023 年 6 月 2 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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::*: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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFinSpaceServiceRolePolicy

描述：允许访问亚马逊 AWS 服务 及其使用或管理的资源的政策 FinSpace

AWSFinSpaceServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 5 月 12 日 16:42 UTC
- 编辑时间：世界标准时间 2023 年 12 月 1 日 21:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFMAdminFullAccess

描述：AWS FM 管理员的完全访问权限

AWSFMAdminFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFMAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 9 日 18:06 UTC
- 编辑时间：2022 年 10 月 20 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFMAdminReadOnlyAccess

描述：AWS FM 管理员的只读访问权限，允许监控 AWS FM 操作

AWSFMAdminReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFMAdminReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2018 年 5 月 9 日 20:07 UTC
- 编辑时间 : 2022 年 10 月 31 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSFMMemberReadOnlyAccess

描述：为 Firewall AWS IAM Manager 成员账户提供对 AWS WAF 操作的只读访问权限

AWSFMMemberReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSFMMemberReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 9 日 21:05 UTC
- 编辑时间：2018 年 5 月 9 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
    },
  ],
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSForWordPressPluginPolicy

描述：适用于 Wordpress 插件 AWS 的托管策略

AWSForWordPressPluginPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSForWordPressPluginPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 30 日 00:27 UTC
- 编辑时间：2020 年 1 月 20 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGitSyncServiceRolePolicy

描述：允许 AWS Code Connections 同步你的 git 存储库中的内容的策略

AWSGitSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 16 日 17:05 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 18:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlobalAcceleratorSLRPolicy

描述：授予 AWS 全球加速器管理 EC2 弹性网络接口和安全组权限的策略。

AWSGlobalAcceleratorSLRPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 4 月 5 日 19:39 UTC
- 编辑时间：2023 年 9 月 12 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "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/*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueConsoleFullAccess

描述：提供通过 AWS Glue 的完全访问权限 AWS Management Console

AWSGlueConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 7 月 14 日 14:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueConsoleSageMakerNotebookFullAccess

描述：提供通过 AWS Glue 的完全访问权限 AWS Management Console 和对 sagemaker 笔记本实例的访问权限。

AWSGlueConsoleSageMakerNotebookFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueConsoleSageMakerNotebookFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 5 日 17:52 UTC
- 编辑时间：2021 年 7 月 15 日 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AwsGlueDataBrewFullAccessPolicy

描述：提供 DataBrew 通过 AWS Glue 的完全访问权限 AWS Management Console。同时，还提供对相关服务（例如 S3、KMS、Glue）的部分访问权限。

AwsGlueDataBrewFullAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AwsGlueDataBrewFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 11 日 16:51 UTC
- 编辑时间：2022 年 2 月 4 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueDataBrewServiceRole

描述：此策略授予 glue 对用户的 glue 数据目录执行操作的权限，该策略还授予 ec2 操作权限，允许 glue 创建 ENI 以连接 VPC 中的资源，还允许 glue 访问 lakeformation 中的注册数据以及访问用户的 cloudwatch 的权限

AWSGlueDataBrewServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueDataBrewServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2020 年 12 月 4 日 21:26 UTC
- 编辑时间：世界标准时间 2024 年 3 月 20 日 23:28
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:BatchGetCustomEntityType",
        "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-*"
}
]
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueSchemaRegistryFullAccess

描述：提供对 AWS Glue 架构注册服务的完全访问权限

AWSGlueSchemaRegistryFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueSchemaRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 00:19 UTC
- 编辑时间：2020 年 11 月 20 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueSchemaRegistryReadOnlyAccess

描述：提供对 AWS Glue 架构注册表服务的只读访问权限

AWSGlueSchemaRegistryReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueSchemaRegistryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 00:20 UTC
- 编辑时间：2020 年 11 月 20 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueServiceNotebookRole

描述：允许客户管理笔记本服务器的 AWS Glue 服务角色策略

AWSGlueServiceNotebookRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGlueServiceNotebookRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 10 月 9 日 15:59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueServiceRole

描述：Glue 服务角色 AWS 的策略，该策略允许访问相关服务，包括 EC2、S3 和 Cloudwatch Logs

AWSGlueServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSGlueServiceRole` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 9 月 11 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AwsGlueSessionUserRestrictedNotebookPolicy

描述：提供权限，允许用户仅创建和使用与用户关联的笔记本会话。此策略还包括明确允许用户传递受限 Glue 会话角色的权限。

AwsGlueSessionUserRestrictedNotebookPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AwsGlueSessionUserRestrictedNotebookPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 18 日 15:24 UTC
- 编辑时间：世界标准时间 2023 年 11 月 22 日 01:32
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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:TagResource",
      "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*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

描述：提供对除会话之外的所有 AWS Glue 资源的完全访问权限。允许用户仅创建和使用与用户关联的笔记本会话。此政策还包括 AWS Glue 在其他 AWS 服务中管理 Glue 资源所需的其他权限。

AwsGlueSessionUserRestrictedNotebookServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AwsGlueSessionUserRestrictedNotebookServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 18 日 15:27 UTC
- 编辑时间：2022 年 4 月 18 日 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
        ]
      }
    }
  },
  {
    "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:TagResource",
    "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AwsGlueSessionUserRestrictedPolicy

描述：提供权限，允许用户仅创建和使用与用户关联的交互式会话。此策略还包括明确允许用户传递受限 Glue 会话角色的权限。

AwsGlueSessionUserRestrictedPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AwsGlueSessionUserRestrictedPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 14 日 21:31 UTC
- 编辑时间：世界标准时间 2024 年 4 月 29 日 22:45
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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:TagResource",
    "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AwsGlueSessionUserRestrictedServiceRole

描述：提供对除会话之外的所有 AWS Glue 资源的完全访问权限。允许用户仅创建和使用与用户关联的交互式会话。此策略还包括 AWS Glue 在其他 AWS 服务中管理 Glue 资源所需的其他权限

AwsGlueSessionUserRestrictedServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AwsGlueSessionUserRestrictedServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 14 日 21:30 UTC
- 编辑时间：世界标准时间 2024 年 4 月 29 日 22:51
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:user}"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{

```

```
"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:TagResource",
    "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGrafanaAccountAdministrator

描述：提供在 Amazon Grafana 中为整个组织创建和管理工作空间的访问权限。

AWSGrafanaAccountAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGrafanaAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 23 日 00:20 UTC
- 编辑时间：2022 年 2 月 15 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGrafanaConsoleReadOnlyAccess

描述：在 Amazon Grafana 中访问只读操作。

AWSGrafanaConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGrafanaConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 2 月 23 日 00:10 UTC
- 编辑时间：2022 年 2 月 15 日 22:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGrafanaWorkspacePermissionManagement

描述：仅提供更新 AWS Grafana 工作空间的用户和群组权限的功能。

AWSGrafanaWorkspacePermissionManagement 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGrafanaWorkspacePermissionManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 23 日 00:15 UTC
- 编辑时间：2023 年 3 月 15 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGrafanaWorkspacePermissionManagementV2

描述：提供更新亚马逊托管 Grafana 工作空间的 IAM 身份中心 (IdC) 用户和群组权限的功能。

AWSGrafanaWorkspacePermissionManagementV2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGrafanaWorkspacePermissionManagementV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：世界标准时间 2024 年 1 月 5 日 18:39
- 编辑时间：世界标准时间 2024 年 1 月 5 日 18:39
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"    
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGreengrassFullAccess

描述：此策略提供对 AWS Greengrass 配置、管理和部署操作的完全访问权限

AWSGreengrassFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGreengrassFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 5 月 3 日 00:47 UTC
- 编辑时间：2017 年 5 月 3 日 00:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGreengrassReadOnlyAccess

描述：此策略提供对 AWS Greengrass 配置、管理和部署操作的只读访问权限

AWSGreengrassReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGreengrassReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 30 日 16:01 UTC
- 编辑时间：2018 年 10 月 30 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGreengrassResourceAccessRolePolicy

描述：AWS Greengrass 服务角色的策略，该策略允许访问相关服务，包括 Lambda AWS 和物联网事物影子。AWS

AWSGreengrassResourceAccessRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSGreengrassResourceAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 2 月 14 日 21:17 UTC
- 编辑时间：2018 年 11 月 14 日 00:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGroundStationAgentInstancePolicy

描述：提供使用 G AWS round Station Agent 的 Dataflow Endpoint 实例权限

AWSGroundStationAgentInstancePolicy是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSGroundStationAgentInstancePolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 29 日 15:23 UTC
- 编辑时间：2023 年 3 月 29 日 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSHealth_EventProcessorServiceRolePolicy

描述：允许 AWS Health 启用 Health 事件处理器功能。

AWSHealth_EventProcessorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 1 月 13 日 19:24 UTC
- 编辑时间：2023 年 1 月 13 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSHealthFullAccess

描述：允许完全访问 AWS 健康 Api 和通知以及 Personal Health Dashboard

AWSHealthFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSHealthFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 6 日 12:30 UTC

- 编辑时间：2020 年 11 月 16 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSHealthImagingFullAccess

描述：提供对 Health AWS h Imaging 服务的完全访问权限。

AWSHealthImagingFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSHealthImagingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 23:39 UTC
- 编辑时间：2023 年 7 月 25 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSHealthImagingReadOnlyAccess

描述：提供对 Health AWS h Imaging 服务的只读访问权限。

AWSHealthImagingReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSHealthImagingReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 23:40 UTC
- 编辑时间：2023 年 8 月 1 日 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIAMIdentityCenterAllowListForIdentityContext

描述：提供允许在 IAM Identity Center 身份上下文中担任的角色执行的操作列表。AWS 安全令牌服务 (AWS STS) 会自动将此策略附加到代入的角色。身份上下文作为 `ProvidedContext` 传递。

`AWSIAMIdentityCenterAllowListForIdentityContext` 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIAMIdentityCenterAllowListForIdentityContext` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 11 月 8 日 15:21 UTC
- 编辑时间：世界标准时间 2024 年 5 月 16 日 22:01
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "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",
```

```
"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",
"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",
    "qbusiness:Chat",
    "qbusiness:ChatSync",
    "qbusiness:ListConversations",
    "qbusiness:ListMessages",
    "qbusiness>DeleteConversation",
    "qbusiness:PutFeedback",
    "sts:SetContext"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIdentitySyncFullAccess

描述：授予对身份同步服务的完全访问权限

AWSIdentitySyncFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSIdentitySyncFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 3 月 23 日 23:29 UTC
- 编辑时间：2022 年 3 月 23 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIdentitySyncReadOnlyAccess

描述：对身份同步服务的只读访问权限

AWSIdentitySyncReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIdentitySyncReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 3 月 23 日 23:29 UTC
- 编辑时间：2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSImageBuilderFullAccess

描述：提供对所有 AWS Image Builder 操作的完全访问权限以及对相关 AWS 服务的资源范围访问权限。

AWSImageBuilderFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSImageBuilderFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 20 日 18:25 UTC
- 编辑时间：2021 年 4 月 13 日 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSImageBuilderReadOnlyAccess

描述：提供对所有 AWS Image Builder 操作的只读权限。

AWSImageBuilderReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSImageBuilderReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 19 日 22:29 UTC
- 编辑时间：2019 年 12 月 19 日 22:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSImportExportFullAccess

描述：提供对在下创建的作业的读写权限 AWS 账户。

AWSImportExportFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSImportExportFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSImportExportReadOnlyAccess

描述：提供对在下创建的作业的只读访问权限 AWS 账户。

AWSImportExportReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSImportExportReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

描述：向事件管理员授予调用其他 AWS 服务的权限，以此作为管理事件的一部分。

AWSIncidentManagerIncidentAccessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIncidentManagerIncidentAccessServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 11 月 13 日 00:01 UTC
- 编辑时间：世界标准时间 2024 年 2 月 20 日 23:02
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
"Statement" : [
  {
    "Sid" : "IncidentAccessPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResources",
      "codedeploy:BatchGetDeployments",
      "codedeploy:ListDeployments",
      "codedeploy:ListDeploymentTargets",
      "autoscaling:DescribeAutoScalingInstances"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIncidentManagerResolverAccess

描述：此策略授予启动、查看和更新事件的权限，并授予对自定义时间轴事件和相关项目的完全访问权限。可将此策略分配给将创建和解决事件的用户。

AWSIncidentManagerResolverAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSIncidentManagerResolverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 10 日 06:12 UTC

- 编辑时间：2021 年 5 月 10 日 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIncidentManagerServiceRolePolicy

描述：此政策授予事件经理代表您管理事件记录和相关资源的权限。

AWSIncidentManagerServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 10 日 03:34 UTC
- 编辑时间：2022 年 12 月 5 日 02:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoT1ClickFullAccess

描述：提供对 AWS IoT 1-Click 的完全访问权限。

AWSIoT1ClickFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoT1ClickFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 11 日 22:10 UTC
- 编辑时间：2018 年 5 月 11 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Action" : [
      "iot1click:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoT1ClickReadOnlyAccess

描述：提供对 AWS IoT 1-Click 的只读访问权限。

AWSIoT1ClickReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoT1ClickReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 11 日 21:49 UTC
- 编辑时间：2018 年 5 月 11 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTAnalyticsFullAccess

描述：提供对 IoT Analytics 的完全访问权限。

AWSIoTAnalyticsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 6 月 18 日 23:02 UTC
- 编辑时间：2018 年 6 月 18 日 23:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTAnalyticsReadOnlyAccess

描述：提供对 IoT Analytics 的只读访问权限。

AWSIoTAnalyticsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIoTAnalyticsReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 18 日 21:37 UTC
- 编辑时间：2018 年 6 月 18 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTConfigAccess

描述：此策略提供对 AWS IoT 配置操作的完全访问权限

AWSIoTConfigAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTConfigAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 27 日 21:52 UTC
- 编辑时间：2019 年 9 月 27 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTConfigReadOnlyAccess

描述：此策略提供对 AWS 物联网配置操作的只读访问权限

AWSIoTConfigReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTConfigReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 27 日 21:52 UTC
- 编辑时间：2019 年 9 月 27 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDataAccess

描述：此策略提供对 AWS IoT 消息操作的完全访问权限

AWSIoTDataAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDataAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 27 日 21:51 UTC
- 编辑时间：2021 年 6 月 23 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

描述：提供对物联网事物组的写入权限和对物联网证书的读取权限，以执行 ADD_THINGS_TO_THING_GROUP 缓解操作

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:55 UTC
- 编辑时间：2019 年 8 月 7 日 17:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderAudit

描述：提供物联网和相关资源的读取权限

AWSIoTDeviceDefenderAudit 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderAudit 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 7 月 18 日 21:17 UTC
- 编辑时间：2019 年 11 月 25 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
  "*"
]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

描述：提供启用物联网日志以执行 ENABLE_IOT_LOGGING 缓解操作的访问权限

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC
- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "iot.amazonaws.com"
      ]
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

描述：提供消息发布对 SNS 主题的访问权限，以执行 PUBLISH_FINDING_TO_SNS 缓解措施

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC

- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

描述：为执行 REPLACE_DEFAULT_POLICY_VERSION 缓解操作提供对物联网策略的写入权限

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC
- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

描述：为执行 UPDATE_CA_CERTIFICATE 缓解操作提供对物联网 CA 证书的写入权限

AWSIoTDeviceDefenderUpdateCACertMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderUpdateCACertMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:05 UTC
- 编辑时间：2019 年 8 月 7 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iot:UpdateCACertificate"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

描述：提供对物联网证书的写入权限，以执行 UPDATE_DEVICE_CERTIFICATE 缓解操作

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:06 UTC
- 编辑时间：2019 年 8 月 7 日 17:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

描述：允许 AWS 物联网设备测试人员访问包括物联网、S3 和 IAM 在内的服务，从而运行 FreeRTOS 资格套件

AWSIoTDeviceTesterForFreeRTOSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIoTDeviceTesterForFreeRTOSFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 2 月 12 日 20:33 UTC
- 编辑时间：2023 年 8 月 10 日 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTDeviceTesterForGreengrassFullAccess

描述：允许 AWS 物联网设备测试人员通过允许访问相关服务（包括 Lambda、IoT、API Gateway、IAM）来运行 Greengrass 资格套件 AWS

AWSIoTDeviceTesterForGreengrassFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIoTDeviceTesterForGreengrassFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 2 月 20 日 21:21 UTC
- 编辑时间：2020 年 6 月 25 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTEventsFullAccess

描述：提供对 IoT Events 的完全访问权限。

AWSIoTEventsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTEventsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 10 日 22:51 UTC
- 编辑时间：2019 年 1 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTEventsReadOnlyAccess

描述：提供对 IoT Events 的只读访问权限。

AWSIoTEventsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTEventsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 10 日 22:50 UTC
- 编辑时间：2019 年 9 月 23 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoT FleetHubFederationAccess

描述：物联网舰队中心应用程序的联邦访问权限

AWSIoT FleetHubFederationAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoT FleetHubFederationAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 15 日 08:08 UTC
- 编辑时间：2022 年 4 月 4 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoT FleetwiseServiceRolePolicy

描述：为辅助功能使用或管理的 AWS 资源和元数据授予权限 AWSIoT Fleetwise

AWSIoT FleetwiseServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 21 日 23:27 UTC
- 编辑时间：2022 年 9 月 21 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoT FleetwiseServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTFullAccess

描述：此策略提供对 AWS 物联网配置和消息传递操作的完全访问权限

AWSIoTFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIoTFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 8 日 15:19 UTC
- 编辑时间：2022 年 5 月 19 日 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTLogging

描述：允许创建 Amazon CloudWatch Log 群组并将日志流式传输到这些群组

AWSIoTLogging是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTLogging 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 10 月 8 日 15:17 UTC
- 编辑时间：2015 年 10 月 8 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
```

```
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTOTAUpdate

描述：允许访问创建 AWS IoT Job 和描述 AWS 代码签名者作业

AWSIoTOTAUpdate 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTOTAUpdate 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 12 月 20 日 20:36 UTC
- 编辑时间：2017 年 12 月 20 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTRoboRunnerFullAccess

描述：此策略授予允许完全访问 AWS IoT 的权限 RoboRunner。

AWSIoTRoboRunnerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTRoboRunnerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 03:54 UTC

- 编辑时间：2023 年 2 月 23 日 18:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTRoboRunnerReadOnly

描述：此策略授予允许对 AWS IoT 进行只读访问的权限 RoboRunner。

AWSIoTRoboRunnerReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTRoboRunnerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 03:43 UTC
- 编辑时间：2022 年 11 月 16 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"    
  }  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTRoboRunnerServiceRolePolicy

描述：允许 AWS IoT RoboRunner 代表客户管理相关 AWS 资源。

AWSIoTRoboRunnerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 2 月 21 日 16:56 UTC
- 编辑时间：2023 年 2 月 21 日 16:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTRuleActions

描述：允许访问 AWS IoT 规则操作支持的所有 AWS 服务

AWSIoTRuleActions 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTRuleActions 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 10 月 8 日 15:14 UTC

- 编辑时间：2018 年 1 月 16 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTSiteWiseConsoleFullAccess

描述：提供 SiteWise 使用管理 AWS 物联网的完全访问权限 AWS Management Console。请注意，此政策还授予创建和列出用于物联网的数据存储的权限 SiteWise（例如 AWS IoT Analytics）、列出和查看 AWS IoT Greengrass 资源、列出和修改 Secrets AWS Manager 机密、检索 AWS 物联网事物影子、列出带有特定标签的资源以及为物联网创建和使用服务相关角色的权限。AWS SiteWise

AWSIoTSiteWiseConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTSiteWiseConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 31 日 21:37 UTC
- 编辑时间：2019 年 5 月 31 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTSiteWiseFullAccess

描述：提供对物联网的完全访问权限 SiteWise。

AWSIoTSiteWiseFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTSiteWiseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 4 日 20:53 UTC
- 编辑时间：2018 年 12 月 4 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTSiteWiseMonitorPortalAccess

描述：此策略授予访问 AWS 物联网 SiteWise 资产和资产数据、创建 AWS IoT M SiteWise onitor 资源和列出 AWS SSO 用户的权限。

AWSIoTSiteWiseMonitorPortalAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTSiteWiseMonitorPortalAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 5 月 19 日 20:01 UTC
- 编辑时间：2020 年 5 月 19 日 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

描述：此角色授予 AWS 物联网 SiteWise 监控者访问您的物 AWS 联网 SiteWise 资产和资产属性的权限，以及通过 AWS 物联网 SiteWise 门户创建 AWS IoT Sitewise 项目、仪表板和访问策略的权限。

AWSIoTSiteWiseMonitorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 14 日 00:59 UTC
- 编辑时间：2019 年 12 月 13 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTSiteWiseReadOnlyAccess

描述：提供对物联网的只读访问权限 SiteWise。

AWSIoTSiteWiseReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTSiteWiseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 4 日 20:55 UTC
- 编辑时间：2022 年 9 月 16 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTThingsRegistration

描述：此策略允许用户使用 AWS IoT StartThingRegistrationTask API 批量注册内容

AWSIoTThingsRegistration 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTThingsRegistration 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 12 月 1 日 20:21 UTC
- 编辑时间：2020 年 10 月 5 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTtwinMakerServiceRolePolicy

描述：允许 AWS IoT TwinMaker 代表您调用其他 AWS 服务并同步其资源。

AWSIoTTwinMakerServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 13 日 18:59 UTC
- 编辑时间：2023 年 11 月 13 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessDataAccess

描述：允许对 AWS IoT Wireless 设备访问关联的身份数据。

AWSIoTWirelessDataAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTWirelessDataAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:31 UTC
- 编辑时间：2020 年 12 月 15 日 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "iotwireless:SendDataToWirelessDevice"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessFullAccess

描述：允许关联的身份完全访问所有 AWS IoT Wireless 操作。

AWSIoTWirelessFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTWirelessFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:27 UTC
- 编辑时间：2020 年 12 月 15 日 15:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessFullPublishAccess

描述：提供 IoT Wireless 代表您发布到物联网规则引擎的完全访问权限。

AWSIoTWirelessFullPublishAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTWirelessFullPublishAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:29 UTC

- 编辑时间：2020 年 12 月 15 日 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessGatewayCertManager

描述：允许关联的身份访问权限创建、列出和描述物联网证书

AWSIoTWirelessGatewayCertManager 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSIoTWirelessGatewayCertManager` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:30 UTC
- 编辑时间：2020 年 12 月 15 日 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessLogging

描述：允许关联的身份创建 Amazon CloudWatch Logs 群组并将日志流式传输到这些群组。

AWSIoTWirelessLogging是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTWirelessLogging 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:32 UTC
- 编辑时间：2020 年 12 月 15 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIoTWirelessReadOnlyAccess

描述：允许关联的身份对 AWS 物联网无线进行只读访问。

AWSIoTWirelessReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIoTWirelessReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:28 UTC
- 编辑时间：2020 年 12 月 15 日 15:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIPAMServiceRolePolicy

描述：允许 VPC IP 地址管理器代表您访问 VPC 资源并与 Organizations 集成。

AWSIPAMServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 30 日 19:08 UTC
- 编辑时间：2023 年 11 月 8 日 19:05 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
    "Sid" : "CloudWatchMetricsPublishActions",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/IPAM"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIQContractServiceRolePolicy

描述：由 AWS IQ 用来代表客户执行付款请求

AWSIQContractServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 22 日 19:28 UTC
- 编辑时间：2019 年 8 月 22 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIQFullAccess

描述：提供对 AWS IQ 的完全访问权限

AWSIQFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSIQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 4 日 23:13 UTC
- 编辑时间：2019 年 9 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIQPermissionServiceRolePolicy

描述：允许 AWS IQ 管理由 AWS IQ 专家担任的角色。

AWSIQPermissionServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 22 日 19:36 UTC
- 编辑时间：2019 年 8 月 22 日 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

描述：允许访问 AWS KMS 自定义密钥存储所需的 AWS 服务和资源

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2018 年 11 月 14 日 20:10 UTC
- 编辑时间：2023 年 11 月 10 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

描述：允许 AWS KMS 同步多区域密钥的共享属性。

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 16 日 15:37 UTC
- 编辑时间：2021 年 6 月 16 日 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSKeyManagementServicePowerUser

描述：提供对 AWS 密钥管理服务 (KMS) 的访问。

AWSKeyManagementServicePowerUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSKeyManagementServicePowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2017 年 3 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLakeFormationCrossAccountManager

描述：通过 Lake Formation 提供对 Glue 资源的跨账户访问权限。同时，还授予对其他必需服务（例如组织和资源访问管理器）的读取权限

AWSLakeFormationCrossAccountManager 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLakeFormationCrossAccountManager 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 4 日 20:59 UTC
- 编辑时间：世界标准时间 2024 年 3 月 22 日 18:51

- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
      "StringLike" : {
        "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLakeFormationDataAdmin

描述：授予对 AWS Lake Formation 和相关服务（例如 AWS Glue）的管理权限，以管理数据湖

AWSLakeFormationDataAdmin 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLakeFormationDataAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 8 月 8 日 17:33 UTC
- 编辑时间：世界标准时间 2024 年 3 月 22 日 18:27
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

策略版本

策略版本：v3（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambda_FullAccess

描述：授予对 Lambda 服务、AWS Lambda 控制台功能和其他相关服务的完全访问权限。
AWS

AWSLambda_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambda_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 17 日 21:14 UTC
- 编辑时间：2020 年 11 月 17 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambda_ReadOnlyAccess

描述：授予对 Lambda 服务、AWS Lambda 控制台功能和其他相关服务的只读访问权限。
AWS

AWSLambda_ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambda_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2020 年 11 月 17 日 21:10 UTC
- 编辑时间 : 2023 年 7 月 27 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaBasicExecutionRole

描述：提供对 CloudWatch 日志的写入权限。

AWSLambdaBasicExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaBasicExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:03 UTC
- 编辑时间：2015 年 4 月 9 日 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaDynamoDBExecutionRole

描述：提供对 DynamoDB 流的列表和读取权限以及对日志的写入权限。 CloudWatch

AWSLambdaDynamoDBExecutionRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaDynamoDBExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:09 UTC
- 编辑时间：2015 年 4 月 9 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```



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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaENIManagementAccess

描述：为 Lambda 函数提供管理已启用 VPC 的 Lambda 函数所使用的 ENI（创建、描述、删除）的最低权限。

AWSLambdaENIManagementAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaENIManagementAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 6 日 00:37 UTC
- 编辑时间：2020 年 10 月 1 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaExecute

描述：提供对 S3 的 Put、Get 访问权限和对 CloudWatch 日志的完全访问权限。

AWSLambdaExecute 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaExecute 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaFullAccess

描述：此策略已进入弃用路径。有关指导，请参阅文档：<https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>。提供对 Lambda、S3、DynamoDB、指标和日志的完全访问权限。CloudWatch

AWSLambdaFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2017 年 11 月 27 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaInvocation-DynamoDB

描述：提供对 DynamoDB Streams 的读取权限。

AWSLambdaInvocation-DynamoDB是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaInvocation-DynamoDB 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaKinesisExecutionRole

描述：提供对 Kinesis 流的列表和读取权限以及对日志的写入权限。 CloudWatch

AWSLambdaKinesisExecutionRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 `AWSLambdaKinesisExecutionRole` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:14 UTC
- 编辑时间：2018 年 11 月 19 日 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```



```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaMSKExecutionRole

描述：提供访问 VPC 内的 MSK 集群、管理 VPC 中的 ENI（创建、描述、删除）以及写入日志所需的 CloudWatch 权限。

AWSLambdaMSKExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaMSKExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 11 日 17:35 UTC
- 编辑时间：2022 年 8 月 2 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaReplicator

描述：向 Lambda Replicator 授予跨区域复制函数所需的权限

AWSLambdaReplicator 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 5 月 23 日 17:53 UTC
- 编辑时间：2017 年 12 月 8 日 00:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaRole

描述：AWS Lambda 服务角色的默认策略。

AWSLambdaRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaSQSQueueExecutionRole

描述：提供对 SQS 队列的接收消息、删除消息和读取属性的访问权限，以及对 CloudWatch 日志的写入权限。

AWSLambdaSQSQueueExecutionRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaSQSQueueExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 6 月 14 日 21:50 UTC
- 编辑时间：2018 年 6 月 14 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLambdaVPCAccessExecutionRole

描述：提供访问 VPC 内资源时执行 Lambda 函数的最低权限-创建、描述、删除网络接口以及写入日志的 CloudWatch 权限。

AWSLambdaVPCAccessExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLambdaVPCAccessExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 11 日 23:15 UTC
- 编辑时间：世界标准时间 2024 年 1 月 5 日 22:38
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerConsumptionPolicy

描述：提供权限以允许访问用户拥有 AWS 授权的许可证时需要使用的 License Manager API 操作。

AWSLicenseManagerConsumptionPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSLicenseManagerConsumptionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 8 月 11 日 23:18 UTC

- 编辑时间：2021 年 8 月 11 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

描述：允许 Lic AWS ense Manager Linux 订阅服务代表你管理资源。

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 12 月 20 日 18:54 UTC
- 编辑时间：2022 年 12 月 20 日 18:54 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
  "*"
]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerMasterAccountRolePolicy

描述：Lic AWS ense Manager 服务主账户角色策略

AWSLicenseManagerMasterAccountRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:03 UTC
- 编辑时间：2022 年 5 月 31 日 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```


了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerMemberAccountRolePolicy

描述：License Manager 服务成员账户角色策略

AWSLicenseManagerMemberAccountRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:04 UTC
- 编辑时间：2019 年 11 月 15 日 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerServiceRolePolicy

描述：Lic AWS ense Manager 服务默认角色策略

AWSLicenseManagerServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:02 UTC
- 编辑时间：2021 年 7 月 30 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

描述：允许 AWS License Manager 用户订阅服务代表您管理资源。

AWSLicenseManagerUserSubscriptionsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 30 日 01:17 UTC
- 编辑时间：2022 年 11 月 21 日 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "bz0vcy31ooqlzk5tsash4r1lik",
        "d44g89hc0gp9jdzm99rznthpw",
        "77yzkpa7kveely1tt7wnsdwoc"
      ]
    }
  },
  "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"
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSM2ServicePolicy

描述：允许 AWS M2 代表您管理 AWS 资源。

AWSM2ServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2022 年 6 月 7 日 20:26 UTC
- 编辑时间：2022 年 6 月 7 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSManagedServices_ContactsServiceRolePolicy

描述：允许 M AWS anaged Services 读取 AWS 资源上标签的值

AWSManagedServices_ContactsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 23 日 17:07 UTC
- 编辑时间：2023 年 3 月 23 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"  
      }  
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

描述：AWS Managed Services-管理侦探控制基础设施的策略

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 12 月 19 日 23:11 UTC
- 编辑时间：2022 年 12 月 19 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSManagedServices_EventsServiceRolePolicy

描述：AWS 用于启用 AMS 事件处理器功能的 Managed Services 策略。

AWSManagedServices_EventsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 2 月 7 日 18:41 UTC
- 编辑时间：2023 年 2 月 7 日 18:41 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```


了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSManagedServicesDeploymentToolkitPolicy

描述：允许 M AWS anaged Services 代表您管理部署工具包。

AWSManagedServicesDeploymentToolkitPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 6 月 9 日 18:33 UTC
- 编辑时间：世界标准时间 2024 年 4 月 4 日 20:41
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceAmiIngestion

描述：AWS Marketplace 允许复制您的亚马逊系统映像 (AMI) 以便在上架这些映像 AWS Marketplace AWSMarketplaceAmiIngestion 是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceAmiIngestion 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 25 日 20:55 UTC
- 编辑时间：2020 年 9 月 25 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceDeploymentServiceRolePolicy

描述：AWS Marketplace 允许为您订阅的商品创建和管理卖家部署参数 AWS Marketplace。

AWSMarketplaceDeploymentServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 15 日 23:34 UTC
- 编辑时间：2023 年 11 月 15 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceFullAccess

描述：提供订阅和取消订阅 AWS Marketplace 软件的功能，允许用户从 Marketplace 的“您的软件”页面管理 Marketplace 软件实例，并提供对 EC2 的管理访问权限。

AWSMarketplaceFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 11 日 17:21 UTC
- 编辑时间：2022 年 3 月 4 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish",
    "sns:setTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:*image-build*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "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/*"
    ]
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceGetEntitlements

描述：提供对 AWS Marketplace 权利的读取权限

AWSMarketplaceGetEntitlements 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceGetEntitlements 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 3 月 27 日 19:37 UTC
- 编辑时间：世界标准时间 2024 年 4 月 5 日 01:27
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSMarketplaceGetEntitlements",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceImageBuildFullAccess

描述：提供对 AWS Marketplace 私有镜像构建功能的完全访问权限。除了创建私有映像外，它还提供向映像添加标签、启动和终止 EC2 实例的权限。

AWSMarketplaceImageBuildFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceImageBuildFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 7 月 31 日 23:29 UTC
- 编辑时间：2022 年 3 月 4 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

描述：允许访问许可证管理 AWS 服务 以及由其使用或管理 AWS Marketplace 的资源。

AWSMarketplaceLicenseManagementServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 3 日 08:33 UTC
- 编辑时间：2020 年 12 月 3 日 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceManageSubscriptions

描述：提供订阅和取消订阅软件的 AWS Marketplace 功能

AWSMarketplaceManageSubscriptions 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceManageSubscriptions 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 1 月 19 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceMeteringFullAccess

描述：提供对“AWS Marketplace 计量”的完全访问权限。

AWSMarketplaceMeteringFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceMeteringFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 3 月 17 日 22:39 UTC
- 编辑时间：2016 年 3 月 17 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceMeteringRegisterUsage

描述：提供通过 AWS Marketplace 计量服务注册资源和跟踪使用情况的权限。

AWSMarketplaceMeteringRegisterUsage 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceMeteringRegisterUsage 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 21 日 01:17 UTC
- 编辑时间：2019 年 11 月 21 日 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceProcurementSystemAdminFullAccess

描述：提供对 AWS Marketplace 电子采购集成的所有管理操作的完全访问权限。

AWSMarketplaceProcurementSystemAdminFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceProcurementSystemAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 25 日 13:07 UTC
- 编辑时间：2019 年 6 月 25 日 13:07 UTC
- ARN: arn:aws:iam::aws:policy/
AWSMarketplaceProcurementSystemAdminFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

描述：允许访问采购订单管理 AWS Marketplace 服务。

AWSMarketplacePurchaseOrdersServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 27 日 15:12 UTC
- 编辑时间：2021 年 10 月 27 日 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```


了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceRead-only

描述：提供查看 AWS Marketplace 订阅的功能

AWSMarketplaceRead-only 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceRead-only 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 1 月 19 日 23:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "ec2:DescribeAccountAttributes",
```

```
    "ec2:DescribeAddresses",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow"
},
{
  "Resource" : "*",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:ListBuilds",
    "aws-marketplace:DescribeBuilds",
    "iam:ListRoles",
    "iam:ListInstanceProfiles",
    "sns:GetTopicAttributes",
    "sns:ListTopics"
  ]
},
{
  "Resource" : "*",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:ListPrivateMarketplaceRequests",
    "aws-marketplace:DescribePrivateMarketplaceRequests"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:ListPrivateListings"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

描述：允许访问转售授权 AWS 服务 以及由其使用或管理 AWS Marketplace 的资源。

AWSMarketplaceResaleAuthorizationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 3 月 5 日 18:47
- 编辑时间：世界标准时间 2024 年 3 月 5 日 18:47
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceSellerFullAccess

描述：提供对卖家操作 AWS Marketplace 以及其他 AWS 服务（例如 AMI 管理）的所有操作的完全访问权限。

AWSMarketplaceSellerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceSellerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 2 日 20:40 UTC
- 编辑时间：世界标准时间 2024 年 3 月 15 日 16:09
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

策略版本

策略版本：v11（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Sid" : "MarketplaceManagement",
"Effect" : "Allow",
"Action" : [
  "aws-marketplace-management:uploadFiles",
  "aws-marketplace-management:viewMarketing",
  "aws-marketplace-management:viewReports",
  "aws-marketplace-management:viewSupport",
  "aws-marketplace-management:viewSettings",
  "aws-marketplace:ListChangeSets",
  "aws-marketplace:DescribeChangeSet",
  "aws-marketplace:StartChangeSet",
  "aws-marketplace:CancelChangeSet",
  "aws-marketplace:ListEntities",
  "aws-marketplace:DescribeEntity",
  "aws-marketplace:ListTasks",
  "aws-marketplace:DescribeTask",
  "aws-marketplace:UpdateTask",
  "aws-marketplace:CompleteTask",
  "aws-marketplace:GetSellerDashboard",
  "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"
    ],
    "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceSellerProductsFullAccess

描述：为卖家提供 AWS Marketplace 管理产品页面和其他 AWS 服务（例如 AMI 管理）的完全访问权限。

AWSMarketplaceSellerProductsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceSellerProductsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 2 日 21:06 UTC
- 编辑时间：2023 年 7 月 18 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

策略版本

策略版本：v7（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "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/*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceSellerProductsReadOnly

描述：为卖家提供 AWS Marketplace 管理商品页面的只读访问权限。

AWSMarketplaceSellerProductsReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMarketplaceSellerProductsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 2 日 21:40 UTC
- 编辑时间：2022 年 11 月 19 日 00:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
```

```
    "aws-marketplace:DescribeEntity",
    "aws-marketplace:ListTasks",
    "aws-marketplace:DescribeTask",
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:ListTagsForResource"
  ],
  "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMediaConnectServicePolicy

描述：允许访问 AWS 服务 以及由其使用或管理的资源的默认策略 MediaConnect。

AWSMediaConnectServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 3 日 22:11 UTC

- 编辑时间：2023 年 4 月 3 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMediaTailorServiceRolePolicy

描述：允许访问使用或管理的 AWS 资源 MediaTailor

AWSMediaTailorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2021 年 9 月 17 日 22:27 UTC
- 编辑时间 : 2021 年 9 月 17 日 22:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubDiscoveryAccess

描述： 策略 AWSMigrationHubService 允许 AWSApplicationDiscoveryService 代表客户致电。

AWSMigrationHubDiscoveryAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubDiscoveryAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:30 UTC
- 编辑时间：2020 年 8 月 6 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubDMSAccess

描述：数据库迁移服务的策略，即在客户账户中扮演角色以调用 Migration Hub

AWSMigrationHubDMSAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubDMSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 14:00 UTC
- 编辑时间：2019 年 10 月 7 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubFullAccess

描述：为客户提供对 Migration Hub 服务的访问权限的托管策略

AWSMigrationHubFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 14:02 UTC
- 编辑时间：2019 年 6 月 19 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubOrchestratorConsoleFullAccess

描述：提供对 Migration Hub、App AWS lic AWS ation Discovery Service、Amazon Simple Service 和 S AWS ecrets Manager 的有限访问 该政策还授予对 Migration Hub Orchestrator 服务的完全访问权限。AWS

AWSMigrationHubOrchestratorConsoleFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubOrchestratorConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:26 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 17:34
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MH0",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
```



```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListAllMyBuckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Sid" : "S3MH0",
    "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*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

描述：需要为 SAP 和 MGN 迁移的实例附加此策略，以便我们的服务通过从 S3 下载脚本来编排实例，并在 EC2 实例中获取机密值。

AWSMigrationHubOrchestratorInstanceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubOrchestratorInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:43 UTC
- 编辑时间：2022 年 4 月 20 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/
AWSMigrationHubOrchestratorInstanceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubOrchestratorPlugin

描述：为 Migration Hub Orchestrator 提供对亚马逊简单存储服务、S AWS secrets Manager 和插件相关操作的 AWS 有限访问权限。

AWSMigrationHubOrchestratorPlugin是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubOrchestratorPlugin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:25 UTC
- 编辑时间：2022 年 4 月 20 日 02:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubOrchestratorServiceRolePolicy

描述：为 Migration Hub Orchestrator 提供迁移本地工作负载并对其进行现代化改造所需的权限

AWSMigrationHubOrchestratorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 4 月 20 日 02:24 UTC
- 编辑时间：世界标准时间 2024 年 3 月 4 日 18:25

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

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    }
  }
}
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

描述：授予对 Migration Hub 重构空间和其他 AWS 相关服务的完全访问权限，但使用没有网桥的环境时不需要的 T AWS ransit Gateway 和 EC2 安全组除外。AWS 该策略还排除 AWS Lambda 和 Res AWS ource Access Manager 所需的权限，因为可以根据标签来缩小它们的范围。

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 3 日 20:09 UTC
- 编辑时间：世界标准时间 2024 年 4 月 11 日 18:16
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-
n1b-*",
    "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"
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

描述：在传递给 SSM Automation 文档的 IAM 服务角色中使用 AWSRefactorSpaces-CreateResources 授予运行自动化所需的权限。此策略授予对 EC2 标签的读取/写入权限，以跟踪自动化进度。启用 Refactor Spaces 环境的网桥后，自动化还会将环境的安全组添加到 EC2 实例，以允许来自环境中其他 Refactor Spaces 服务的流量。此策略还授予 Application Migration Service 的启动后操作 SSM 参数的访问权限。

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 10 日 15:08 UTC

- 编辑时间：2023 年 8 月 10 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-
**
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubRefactorSpacesFullAccess

描述：授予对 AWS MigrationHub 重构空间、AWS MigrationHub 重构空间控制台功能和其他相关 AWS 服务的完全访问权限，但 Lambda AWS 和 Res AWS ource Access Manager 所需的权限除外，因为它们可以根据标签进行范围缩小。

AWSMigrationHubRefactorSpacesFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSMigrationHubRefactorSpacesFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 07:12 UTC
- 编辑时间：世界标准时间 2024 年 4 月 11 日 17:45
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
    }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

描述：提供对 Migration Hub 重构空间管理或使用的 AWS AWS 资源的访问权限。

AWSMigrationHubRefactorSpacesServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 29 日 06:50 UTC
- 编辑时间：2023 年 7 月 20 日 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubSMSAccess

描述：服务器迁移服务在客户账户中扮演角色以调用 Migration Hub 的政策

AWSMigrationHubSMSAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubSMSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:57 UTC
- 编辑时间：2019 年 10 月 7 日 18:01 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubStrategyCollector

描述：授予权限以允许与 Migration Hub 策略建议服务进行通信、对与该 AWS 服务相关的 S3 存储桶进行读/写访问权限、向其上传日志和指标的 Amazon API Gateway、S AWS secrets Manager 获取证书的访问权限以及任何相关服务。AWS

AWSMigrationHubStrategyCollector 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubStrategyCollector 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 19 日 20:15 UTC
- 编辑时间：世界标准时间 2024 年 4 月 1 日 16:21
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubStrategyConsoleFullAccess

描述：授予对 Migrati AWS on Hub 策略建议服务的完全访问权限以及通过访问相关 AWS 服务的权限 AWS Management Console。

AWSMigrationHubStrategyConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMigrationHubStrategyConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 19 日 20:13 UTC
- 编辑时间：2022 年 11 月 9 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubStrategyServiceRolePolicy

描述：允许访问由 AWS Migration Hub 策略建议服务使用或管理的 AWS 资源。

AWSMigrationHubStrategyServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型：**服务相关角色策略
- **创建时间：**2021 年 10 月 19 日 20:02 UTC
- **编辑时间：**2021 年 10 月 19 日 20:02 UTC
- **ARN:** `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

策略版本

策略版本： v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMobileHub_FullAccess

描述：此策略可以附加到任何用户、角色或组，以授予用户在 M AWS obile Hub 中创建、删除和修改项目（及其关联 AWS 资源）的权限。这还包括为每个 Mobile Hub 项目生成和下载示例移动应用程序源代码的权限。

AWSMobileHub_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMobileHub_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 5 日 19:56 UTC
- 编辑时间：2019 年 12 月 19 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMobileHub_ReadOnly

描述：此策略可以附加到任何用户、角色或组，以授予用户在 M AWS obile Hub 中列出和查看项目的权限。这还包括为每个 Mobile Hub 项目生成和下载示例移动应用程序源代码的权限。它不允许用户修改任何 Mobile Hub 项目的任何配置。

AWSMobileHub_ReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSMobileHub_ReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 5 日 19:55 UTC
- 编辑时间：2018 年 7 月 23 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMSKReplicatorExecutionRole

描述：向 Amazon MSK Replicator 授予在 MSK 集群之间复制数据的权限。

AWSMSKReplicatorExecutionRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSMSKReplicatorExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 00:07
- 编辑时间：世界标准时间 2024 年 3 月 25 日 21:36
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSNetworkFirewallServiceRolePolicy

描述：AWSNetworkFirewall 允许创建和管理防火墙所需的资源。

AWSNetworkFirewallServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 17 日 17:17 UTC
- 编辑时间：2023 年 3 月 30 日 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSNetworkManagerCloudWANServiceRolePolicy

描述： NetworkManager 允许访问与您的核心网络相关的资源

AWSNetworkManagerCloudWANServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 12 日 12:17 UTC
- 编辑时间：2022 年 7 月 12 日 12:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSNetworkManagerFullAccess

描述：提供 NetworkManager 通过 Amazon 的完全访问权限 AWS Management Console。

AWSNetworkManagerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSNetworkManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 17:37 UTC
- 编辑时间：2019 年 12 月 3 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSNetworkManagerReadOnlyAccess

描述：NetworkManager 通过提供对 Amazon 的只读访问权限 AWS Management Console。

AWSNetworkManagerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSNetworkManagerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 17:35 UTC
- 编辑时间：2019 年 12 月 3 日 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "networkmanager:Describe*",
      "networkmanager:Get*",
      "networkmanager:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSNetworkManagerServiceRolePolicy

描述：NetworkManager 允许访问与您的全球网络相关的资源

AWSNetworkManagerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 14:03 UTC
- 编辑时间：2022 年 7 月 27 日 19:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorks_FullAccess

描述：提供对的完全访问权限 AWS OpsWorks。

AWSOpsWorks_FullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorks_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 16:29 UTC
- 编辑时间：2021 年 1 月 22 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksCloudWatchLogs

描述：使启用了 CWLogs 集成的 OpsWorks 实例能够传送日志和创建所需的日志组

AWSOpsWorksCloudWatchLogs 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 3 月 30 日 17:47 UTC
- 编辑时间：2017 年 3 月 30 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksCMInstanceProfileRole

描述：为 OpsWorks CM 启动的实例提供 S3 访问权限。

AWSOpsWorksCMInstanceProfileRole是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksCMInstanceProfileRole 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 24 日 09:48 UTC
- 编辑时间：2021 年 4 月 23 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksCMServiceRole

描述：用于创建 OpsWorks CM 服务器的服务角色策略。

AWSOpsWorksCMServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksCMServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 11 月 24 日 09:49 UTC
- 编辑时间：2021 年 4 月 23 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksInstanceRegistration

描述：为 Amazon EC2 实例提供向 AWS OpsWorks 堆栈注册的权限。

AWSOpsWorksInstanceRegistration 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksInstanceRegistration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 6 月 3 日 14:23 UTC
- 编辑时间：2016 年 6 月 3 日 14:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "opsworks:DescribeStacks",
    "opsworks:RegisterInstance"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksRegisterCLI_EC2

描述：允许通过 OpsWorks CLI 注册 EC2 实例的策略

AWSOpsWorksRegisterCLI_EC2 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksRegisterCLI_EC2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 18 日 15:56 UTC
- 编辑时间：2019 年 6 月 18 日 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOpsWorksRegisterCLI_OnPremises

描述：允许通过 OpsWorks CLI 注册本地实例的策略

AWSOpsWorksRegisterCLI_OnPremises 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOpsWorksRegisterCLI_OnPremises 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 18 日 15:33 UTC
- 编辑时间：2019 年 6 月 18 日 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
}
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOrganizationsFullAccess

描述：提供对 Organizations 的 AWS 完全访问权限。

AWSOrganizationsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOrganizationsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 6 日 20:31 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 17:49
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOrganizationsReadOnlyAccess

描述：提供对 Organizations 的 AWS 只读权限。

AWSOrganizationsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOrganizationsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 6 日 20:32 UTC
- 编辑时间：世界标准时间 2024 年 6 月 7 日 21:32
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOrganizationsServiceTrustPolicy

描述：一项政策，允许 AWS Organizations 与其他经批准 AWS 服务的组织共享信任，目的是简化客户配置。

AWSOrganizationsServiceTrustPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 10 日 23:04 UTC
- 编辑时间：2017 年 11 月 1 日 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOutpostsAuthorizeServerPolicy

描述：此策略授予的权限允许您在本地网络上安装 Outpost 服务器。

AWSOutpostsAuthorizeServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSOutpostsAuthorizeServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 4 日 19:23 UTC
- 编辑时间：2023 年 1 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "outposts:StartConnection",
        "outposts:GetConnection"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOutpostsServiceRolePolicy

描述：服务关联角色策略允许访问由 AWS Outposts 管理的资源

AWSOutpostsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 9 日 22:55 UTC
- 编辑时间：2020 年 11 月 9 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaApplianceRolePolicy

描述：允许 AWS Panorama 设备上的 AWS 物联网软件将日志上传到亚马逊 CloudWatch。

AWSPanoramaApplianceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaApplianceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:13 UTC

- 编辑时间：2020 年 12 月 1 日 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaApplianceServiceRolePolicy

描述：允许 AWS Panorama 设备将日志上传到亚马逊 CloudWatch，并作为与 Panor AWS ama 一起使用而创建的 Amazon S3 接入点获取对象。

AWSPanoramaApplianceServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaApplianceServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 10 月 20 日 12:14 UTC
- 编辑时间：2023 年 1 月 17 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
    }
  }
}
]

```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaFullAccess

描述：提供对 P AWS anorama 的完全访问权限

AWSPanoramaFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 13:12 UTC
- 编辑时间：2022 年 1 月 12 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "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"
    }
  }
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaGreengrassGroupRolePolicy

描述：允许 Panor AWS ama 设备上的 Lambda 函数管理 AWS Panorama 中的资源，将日志和指标上传到亚马逊 CloudWatch，以及管理为与 Panorama 一起使用而创建的存储桶中的对象。

AWSPanoramaGreengrassGroupRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaGreengrassGroupRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:10 UTC
- 编辑时间：2021 年 1 月 6 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaSageMakerRolePolicy

描述：允许亚马逊管理专 SageMaker 为 P AWS anorama 使用而创建的存储桶中的对象。

AWSPanoramaSageMakerRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaSageMakerRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2020 年 12 月 1 日 13:13 UTC
- 编辑时间：2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3::*aws-panorama*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaServiceLinkedRolePolicy

描述：允许 AWS Panorama 管理 AWS 物联网、S AWS secrets Manager 和 AWS Panorama 中的资源。

AWSPanoramaServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 20 日 12:12 UTC
- 编辑时间：2021 年 10 月 20 日 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPanoramaServiceRolePolicy

描述：允许 AWS Panorama 管理亚马逊 S3、AWS 物联网、AWS 物联网 GreenGrass、AWS Lambda SageMaker、亚马逊和亚马逊 CloudWatch 日志中的资源，并将服务角色传递给物联网 GreenGrass、AWS 物 AWS 联网和亚马逊。 SageMaker

AWSPanoramaServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSPanoramaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:14 UTC
- 编辑时间：2020 年 12 月 1 日 13:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPriceListServiceFullAccess

描述：提供对 AWS 价目表服务的完全访问权限。

AWSPriceListServiceFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPriceListServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 22 日 00:36 UTC
- 编辑时间：2017 年 11 月 22 日 00:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPRivateCAAuditor

描述：为审核员提供对 AWS 私有证书颁发机构的访问权限

AWSPRivateCAAuditor 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPRivateCAAuditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:33 UTC
- 编辑时间：2023 年 2 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPRivateCAAuditor

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPriateCAFullAccess

描述：提供对 AWS 私有证书颁发机构的完全访问权限

AWSPrivateCAFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPrivateCAFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:20 UTC
- 编辑时间：2023 年 2 月 14 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPriateCAPrivilegedUser

描述：为特权证书用户提供对 AWS 私有证书颁发机构的访问权限

AWSPriateCAPrivilegedUser是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSPriateCAPrivilegedUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:26 UTC
- 编辑时间：2023 年 2 月 14 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAPrivilegedUser

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
```



```
    "StringLike" : {
      "acm-pca:TemplateArn" : [
        "arn:aws:acm-pca:::template/*CACertificate*/V*"
      ]
    }
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition" : {
      "StringNotLike" : {
        "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPRivateCARedOnly

描述：提供对 AWS 私有证书颁发机构的只读访问权限

AWSPRivateCARedOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPRivateCARedOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:30 UTC
- 编辑时间：2023 年 2 月 14 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPRivateCARedOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPriateCAUser

描述：为证书用户提供对 AWS 私有证书颁发机构的访问权限

AWSPriateCAUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPriateCAUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:16 UTC
- 编辑时间：2023 年 2 月 14 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAUser

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPrivateMarketplaceAdminFullAccess

描述：提供对 AWS 私有市场 (Private Marketplace) 所有管理操作的完全访问权限。

AWSPrivateMarketplaceAdminFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPrivateMarketplaceAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 16:32 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:05
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPrivateMarketplaceRequests

描述：提供在 AWS 私有市场 Private Marketplace 中创建请求的权限。

AWSPrivateMarketplaceRequests 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPrivateMarketplaceRequests 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 28 日 21:44 UTC
- 编辑时间：2019 年 10 月 28 日 21:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPrivateNetworksServiceRolePolicy

描述：允许 AWS 专用网络服务代表客户管理资源。

AWSPrivateNetworksServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 12 月 16 日 23:17 UTC
- 编辑时间：2021 年 12 月 16 日 23:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonCodeBuildProvisioningBasicAccess

描述：权限 CodeBuild 需要为 AWS Proton CodeBuild 配置运行构建。

AWSProtonCodeBuildProvisioningBasicAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSProtonCodeBuildProvisioningBasicAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 9 日 21:04 UTC
- 编辑时间：2022 年 11 月 9 日 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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:*:*:*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

描述：允许 AWS Proton 代表您管理使用的 Proton 资源配置 CodeBuild 和其他 AWS 服务。

AWSProtonCodeBuildProvisioningServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2022 年 11 月 9 日 21:32 UTC
- 编辑时间：2023 年 5 月 17 日 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonDeveloperAccess

描述：提供对 AWS Proton API 和管理控制台的访问权限，但不允许管理 Proton 模板或环境。

AWSProtonDeveloperAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSProtonDeveloperAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:02 UTC
- 编辑时间：世界标准时间 2024 年 6 月 6 日 18:26
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonFullAccess

描述：提供对 AWS Proton API 和管理控制台的完全访问权限。除了这些权限外，还需要访问 Amazon S3 才能从 S3 桶注册模板包，以及访问 Amazon IAM 以创建和管理 Proton 的服务角色。

AWSProtonFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSProtonFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:07 UTC
- 编辑时间：世界标准时间 2024 年 6 月 6 日 18:29
- ARN: arn:aws:iam::aws:policy/AWSProtonFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonReadOnlyAccess

描述：提供对 AWS Proton API 和管理控制台的只读访问权限。

AWSProtonReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSProtonReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:09 UTC
- 编辑时间：2022 年 11 月 18 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonServiceGitSyncServiceRolePolicy

描述：允许 AWS Proton 将你的服务、环境和组件定义从 git 存储库同步到 Pro AWS ton 的策略。

AWSProtonServiceGitSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 4 日 15:55 UTC
- 编辑时间：2023 年 4 月 4 日 15:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSProtonSyncServiceRolePolicy

描述：允许 AWS Proton 将你的 git 存储库内容同步到 Proton 或将 Proton 内容同步到你的 git 存储库的政策。

AWSProtonSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 23 日 21:14 UTC
- 编辑时间：世界标准时间 2024 年 5 月 5 日 01:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPurchaseOrdersServiceRolePolicy

描述：授予在账单控制台上查看和修改采购订单的权限

AWSPurchaseOrdersServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSPurchaseOrdersServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 6 日 18:15 UTC
- 编辑时间：2023 年 7 月 17 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightAssetBundleExportPolicy

描述：提供执行 QuickSight 资产包导出操作所需的权限集

AWSQuickSightAssetBundleExportPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightAssetBundleExportPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 3 月 27 日 21:31
- 编辑时间：世界标准时间 2024 年 3 月 27 日 21:31
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:vpccConnection/*"
},
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightAssetBundleImportPolicy

描述：提供执行 QuickSight 资源包导入操作所需的权限集

AWSQuickSightAssetBundleImportPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightAssetBundleImportPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 3 月 27 日 21:40
- 编辑时间：世界标准时间 2024 年 3 月 27 日 21:40
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuicksightAthenaAccess

描述：快速访问用于 Athena 查询结果的 Athena API 和 S3 存储桶

AWSQuicksightAthenaAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuicksightAthenaAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 9 日 02:31 UTC
- 编辑时间：2021 年 7 月 7 日 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightDescribeRDS

描述：QuickSight 允许描述 RDS 资源

AWSQuickSightDescribeRDS 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightDescribeRDS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:24 UTC
- 编辑时间：2015 年 11 月 10 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightDescribeRedshift

描述：允许 QuickSight 描述 Redshift 资源

AWSQuickSightDescribeRedshift 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightDescribeRedshift 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:25 UTC
- 编辑时间：2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightElasticsearchPolicy

描述：提供从亚马逊访问亚马逊 Elasticsearch 资源的权限 QuickSight

AWSQuickSightElasticsearchPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightElasticsearchPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 9 日 17:27 UTC
- 编辑时间：2021 年 9 月 7 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightIoTAnalyticsAccess

描述：授予对 IoT Analytics 数据集的 QuickSight 只读访问权限

AWSQuickSightIoTAnalyticsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightIoTAnalyticsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 17:00 UTC
- 编辑时间：2017 年 11 月 29 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightListIAM

描述：QuickSight 允许列出 IAM 实体

AWSQuickSightListIAM是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightListIAM 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:25 UTC
- 编辑时间：2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuicksightOpenSearchPolicy

描述：提供从亚马逊访问亚马逊 OpenSearch 资源的权限 QuickSight

AWSQuicksightOpenSearchPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuicksightOpenSearchPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 9 月 7 日 23:26 UTC
- 编辑时间：2021 年 9 月 7 日 23:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightSageMakerPolicy

描述：提供从亚马逊访问亚马逊 SageMaker 资源的权限 QuickSight

AWSQuickSightSageMakerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightSageMakerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 1 月 17 日 17:18 UTC
- 编辑时间：2023 年 10 月 30 日 17:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  }
]
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSQuickSightTimestreamPolicy

描述：AWS QuickSight 访问 AWS Timestream API。客户可以将此策略附加到 AWS QuickSight 角色以允许检索数据和元数据。

AWSQuickSightTimestreamPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSQuickSightTimestreamPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：2020 年 9 月 30 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSReachabilityAnalyzerServiceRolePolicy

描述：允许 VPC Reachability Analyzer 代表您访问 AWS 资源并与 Organizations 集成 AWS。

AWSReachabilityAnalyzerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2022 年 11 月 23 日 17:12 UTC
- 编辑时间：世界标准时间 2024 年 5 月 15 日 20:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListCustomRoutingAccelerators",
"globalaccelerator:ListCustomRoutingEndpointGroups",
"globalaccelerator:ListCustomRoutingListeners",
"globalaccelerator:ListCustomRoutingPortMappings",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"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"
    ]
}
]
}
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRefactoringToolkitFullAccess

描述：此策略授予使用微软 Visual Studio 的 .NET 重构工具包扩展插件的 AWS 服务的权限。它旨在附加到本地 AWS 配置文件中。该策略允许上传应用程序构件并从 Amazon S3 下载生成的构件。它允许使用亚马逊弹性容器注册表 (Amazon ECR) Container Registry (Amazon ECR) 中存储 AWS CodeBuild 和检索映像将应用程序构建到容器映像中。它还允许将应用程序部署到亚马逊弹性容器服务 (Amazon ECS) Service AWS 等容器服务、可选创建 VPC 资源、可选连接到目录 AWS 服务等现有基础设施以及其他相关服务。

AWSRefactoringToolkitFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSRefactoringToolkitFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 10 月 25 日 16:41 UTC
- 编辑时间：世界标准时间 2024 年 3 月 25 日 18:43
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "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-*"
  ]
},
{
  "Sid" : "CodeBuildCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild:UpdateProject"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "CodeBuildExecutionAccess",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:StartBuild"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/*"
},
{
  "Sid" : "CreateSecurityGroupAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "Ec2CreateAccess",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateInternetGateway",
  "ec2:CreateKeyPair",
  "ec2:CreateRoute",
  "ec2:CreateRouteTable",
  "ec2:CreateSubnet",
  "ec2:CreateTags",
  "ec2:CreateVpc",
  "ec2:AuthorizeSecurityGroupIngress"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/a2c-generated" : "false"
  }
}
},
{
  "Sid" : "Ec2CreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    }
  }
}
},
{
  "Sid" : "Ec2ModifyAccess",
  "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"
    }
  }
},
{
  "Sid" : "Ec2ModifyAccessATS",
  "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"
    }
  }
},
{
  "Sid" : "EcrCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
```

```
    "ecr:TagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "EcrCreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr:TagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcrModifyAccess",
  "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"
    }
  }
},
{
  "Sid" : "EcrModifyAccessATS",
  "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"
      }
    }
  },
  {
    "Sid" : "EcsCreateAccess",
    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs:CreateService",
      "ecs:RegisterTaskDefinition",
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/a2c-generated" : "false"
      }
    }
  },
  {
    "Sid" : "EcsCreateAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs:CreateService",
      "ecs:RegisterTaskDefinition",
      "ecs:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/application-transformation" : "false"
      }
    }
  }

```

```
    }
  }
},
{
  "Sid" : "EcsModifyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateService",
    "ecs:TagResource",
    "ecs:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "EcsModifyAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateService",
    "ecs:TagResource",
    "ecs:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcsReadTaskDefinitionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:DescribeTaskDefinition"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cloudformation.amazonaws.com"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "EcsExecuteCommandInSidecar",
    "Effect" : "Allow",
    "Action" : [
      "ecs:ExecuteCommand"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ecs:container-name" : "a2c-sidecar"
      }
    }
  },
  {
    "Sid" : "EcsExecuteCommandInSidecarATS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:ExecuteCommand"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ecs:container-name" : "application-transformation-sidecar"
      }
    }
  },
  {
    "Sid" : "CreateEcsServiceLinkedRoleAccess",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "ecs.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudwatchCreateAccess",
    "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"
      ]
    }
  }
},
{
  "Sid" : "CloudwatchCreateAccessATS",
  "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"
      ]
    }
  }
},
{
  "Sid" : "CloudwatchGetAccess",
  "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"
      }
    }
  },
  {
    "Sid" : "CloudwatchGetAccessATS",
    "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"
      }
    }
  },
  {
    "Sid" : "SsmParameterAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:AddTagsToResource",
      "ssm:GetParameters",
      "ssm:PutParameter",
      "ssm:RemoveTagsFromResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
  },
  {
    "Sid" : "SsmMessagesAccess",
    "Effect" : "Allow",

```

```
"Action" : [
  "ssm:DescribeSessions",
  "ssmmessages:CreateControlChannel",
  "ssmmessages:CreateDataChannel",
  "ssmmessages:OpenControlChannel",
  "ssmmessages:OpenDataChannel"
],
"Resource" : "*"
},
{
  "Sid" : "S3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::*/*refactoringtoolkit*",
    "arn:aws:s3::*/*a2c-generated*",
    "arn:aws:s3::*/*application-transformation*"
  ]
},
{
  "Sid" : "S3ListAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3::*:*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : [
        "application-transformation",
        "refactoringtoolkit"
      ]
    }
  }
},
{
  "Sid" : "ReadOnlyAccess",
  "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" : "*"
},
{
  "Sid" : "GetECSSLR",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
},
{
  "Sid" : "PortingAssistantFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ]
},

```

```
"Resource" : [
  "arn:aws:s3::aws.portingassistant.dotnet.datastore",
  "arn:aws:s3::aws.portingassistant.dotnet.datastore/*"
],
{
  "Sid" : "ApplicationTransformationAccess",
  "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" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource" : "arn:aws:kms:*:*:*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "kms:ResourceAliases" : "alias/application-transformation*"
    }
  }
},
{
  "Sid" : "EcrPushAccess",
  "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"
    }
  }
},
{
  "Sid" : "EcrAuthAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:GetAuthorizationToken"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsCreateGrantAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "arn:aws:kms:*:*:*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    },
    "ForAnyValue:StringLike" : {
      "kms:ResourceAliases" : "alias/application-transformation*"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRefactoringToolkitSidecarPolicy

描述：此策略旨在供为测试应用程序而创建的 Amazon ECS 任务使用 Microsoft Visual Studio for AWS io 的 .NET 重构工具包扩展插件。AWS 该策略授予从 Amazon S3 下载应用程序工件、使用 S AWS systems Manager 传达任务状态以及其他所需服务的权限。

AWSRefactoringToolkitSidecarPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSRefactoringToolkitSidecarPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 10 月 25 日 16:41 UTC
- 编辑时间：2022 年 10 月 29 日 22:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSrePostPrivateCloudWatchAccess

描述：提供 re: Post 私密访问权限以发布指标数据 CloudWatch

AWSrePostPrivateCloudWatchAccess是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 15 日 16:37 UTC
- 编辑时间：2023 年 11 月 15 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRepostSpaceSupportOperationsPolicy

描述：此政策允许 re: Post Space 服务创建、管理和解决通过 Space 应用程序创建的支持案例。

AWSRepostSpaceSupportOperationsPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSRepostSpaceSupportOperationsPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 21:52
- 编辑时间：世界标准时间 2023 年 11 月 26 日 21:52
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Sid" : "RepostSpaceSupportOperations",
    "Effect" : "Allow",
    "Action" : [
      "support:AddAttachmentsToSet",
      "support:AddCommunicationToCase",
      "support:CreateCase",
      "support:DescribeCases",
      "support:DescribeCommunications",
      "support:ResolveCase"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResilienceHubAssessmentExecutionPolicy

描述：Resili AWS ence Hub 服务角色的策略，该策略允许访问其他 AWS 服务以执行评估。

AWSResilienceHubAssessmentExecutionPolicy是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSResilienceHubAssessmentExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 12:32 UTC
- 编辑时间：世界标准时间 2024 年 3 月 24 日 18:05

- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
        "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",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperimentTemplate",
"fis:ListExperimentTemplates",
```



```
"fis:ListExperiments",
"fsx:DescribeFileSystems",
"lambda:GetFunctionConcurrency",
"lambda:GetFunctionConfiguration",
"lambda:ListAliases",
"lambda:ListVersionsByFunction",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyTargets",
"rds:DescribeDBSnapshots",
"rds:DescribeGlobalClusters",
"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:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicyStatus",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetMultiRegionAccessPointRoutes",
"s3:GetReplicationConfiguration",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"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" : "AWSResilienceHubS3Statement",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
},
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceAccessManagerFullAccess

描述：提供对 Res AWS ource Access Manager 的完全访问权限

AWSResourceAccessManagerFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceAccessManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 4 日 17:28 UTC
- 编辑时间：2019 年 6 月 4 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceAccessManagerReadOnlyAccess

描述：提供对 Res AWS ource Access Manager 的只读访问权限。

AWSResourceAccessManagerReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceAccessManagerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 9 日 20:58 UTC
- 编辑时间：2019 年 12 月 9 日 20:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceAccessManagerResourceShareParticipantAccess

描述：提供对资源共享参与者所需的 AWS 资源 Access Manager API 的访问权限。

AWSResourceAccessManagerResourceShareParticipantAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceAccessManagerResourceShareParticipantAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 9 日 20:41 UTC
- 编辑时间：2019 年 12 月 9 日 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceAccessManagerServiceRolePolicy

描述：策略包含对客户组织结构的只读 AWS 资源访问权限 Resource Access Manager 访问权限。它还包含自行删除角色的 IAM 权限。

AWSResourceAccessManagerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 14 日 19:28 UTC
- 编辑时间：2018 年 11 月 14 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceExplorerFullAccess

描述：此策略授予访问资源管理器资源的管理权限，并向其他 AWS 服务授予只读权限以支持此访问。

AWSResourceExplorerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceExplorerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 7 日 20:01 UTC
- 编辑时间：2023 年 11 月 14 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceExplorerOrganizationsAccess

描述：此策略向资源管理器授予管理权限，并向其他 AWS 服务授予只读权限以支持此访问权限。AWS Organizations 管理员需要这些权限才能在控制台中设置和管理多账户搜索。

AWSResourceExplorerOrganizationsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceExplorerOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 11 月 14 日 17:01 UTC
- 编辑时间：2023 年 11 月 14 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceExplorerReadOnlyAccess

描述：此策略授予搜索和查看 Resource Explorer 资源的只读权限，并向其他 AWS 服务授予只读权限以支持此访问权限。

AWSResourceExplorerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceExplorerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 7 日 19:56 UTC
- 编辑时间：2023 年 11 月 14 日 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceExplorerServiceRolePolicy

描述：允许资源浏览器代表你查看资源和 CloudTrail 事件，为你的资源编制索引以供搜索。

AWSResourceExplorerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 10 月 25 日 20:35 UTC
- 编辑时间：世界标准时间 2023 年 12 月 20 日 13:58
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "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"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
```

```
"amplifyuibuilder:ListComponents",
"amplifyuibuilder:ListThemes",
"app-integrations:ListEventIntegrations",
"apprunner:ListServices",
"apprunner:ListVpcConnectors",
"appstream:DescribeAppBlocks",
"appstream:DescribeApplications",
"appstream:DescribeFleets",
"appstream:DescribeImageBuilders",
"appstream:DescribeStacks",
"appsync:ListGraphQLApis",
"aps:ListRuleGroupsNamespaces",
"aps:ListWorkspaces",
"athena:ListDataCatalogs",
"athena:ListWorkGroups",
"autoscaling:DescribeAutoScalingGroups",
"backup:ListBackupPlans",
"backup:ListReportPlans",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:ListSchedulingPolicies",
"cloudformation:ListStacks",
"cloudformation:ListStackSets",
"cloudfront:ListCachePolicies",
"cloudfront:ListCloudFrontOriginAccessIdentities",
"cloudfront:ListDistributions",
"cloudfront:ListFieldLevelEncryptionConfigs",
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListOriginRequestPolicies",
"cloudfront:ListRealtimeLogConfigs",
"cloudfront:ListResponseHeadersPolicies",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"codeartifact:ListDomains",
"codeartifact:ListRepositories",
"codebuild:ListProjects",
"codecommit:ListRepositories",
"codeguru-profiler:ListProfilingGroups",
"codepipeline:ListPipelines",
```



```
"codestar-connections:ListConnections",
"cognito-identity:ListIdentityPools",
"cognito-idp:ListUserPools",
"databrew:ListDatasets",
"databrew:ListRecipes",
"databrew:ListRulesets",
"detective:ListGraphs",
"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:DescribeIpams",
"ec2:DescribeIpamScopes",
"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:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetSubnetCidrReservations",
"ecr:DescribeRepositories",
"ecr-public:DescribeRepositories",
"ecs:DescribeCapacityProviders",
"ecs:DescribeServices",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:ListServices",
"ecs:ListTaskDefinitions",
"ecs:ListTasks",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
```

```
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeReservedCacheNodes",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"emr-serverless:ListApplications",
"es:ListDomainNames",
"events:ListEventBuses",
"events:ListRules",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"finspace:ListEnvironments",
"firehose:ListDeliveryStreams",
"fis:ListExperimentTemplates",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"frauddetector:GetEntityTypeTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetLabels",
"frauddetector:GetOutcomes",
"frauddetector:GetVariables",
"gamelift:ListAliases",
"geo:ListPlaceIndexes",
"geo:ListTrackers",
"greengrass:ListComponents",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"glue:GetDatabases",
```

```
"glue:GetJobs",
"glue:GetTables",
"glue:GetTriggers",
"greengrass:ListComponentVersions",
"greengrass:ListGroups",
"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",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iot:ListJobTemplates",
"iot:ListAuthorizers",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListSecurityProfiles",
"iot:ListThings",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListGateways",
```

```
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListWorkspaces",
"kafka:ListConfigurations",
"kms:ListKeys",
"ivs:ListChannels",
"ivs:ListStreamKeys",
"kafka:ListClusters",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisvideo:ListStreams",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"lambda:ListLayers",
"lambda:ListLayerVersions",
"lex:ListBots",
"lex:ListBotAliases",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"lookoutmetrics:ListAlerts",
"lookoutvision:ListProjects",
"mediapackage:ListChannels",
"mediapackage:ListOriginEndpoints",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mq:ListBrokers",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeACLs",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeUsers",
"mobiletargeting:GetApps",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTemplates",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetDevices",
"networkmanager:GetLinks",
```

```
"networkmanager:ListAttachments",
"networkmanager:ListCoreNetworks",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:ListAccounts",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListDelegatedAdministrators",
"panorama:ListPackages",
"personalize:ListDatasetGroups",
"personalize:ListDatasets",
"personalize:ListSchemas",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"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:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"rekognition:DescribeProjects",
```

```
"resiliencyhub:ListApps",
"resiliencyhub:ListResiliencyPolicies",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListViews",
"resource-groups:ListGroups",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53-recovery-readiness:ListRecoveryGroups",
"route53-recovery-readiness:ListResourceSets",
"route53resolver:ListFirewallDomainLists",
"route53resolver:ListFirewallRuleGroups",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverRules",
"s3:GetBucketLocation",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListStorageLensConfigurations",
"sagemaker:ListModels",
"sagemaker:ListNotebookInstances",
"secretsmanager:ListSecrets",
"servicecatalog:ListApplications",
"servicecatalog:ListAttributeGroups",
"signer:ListSigningProfiles",
"sns:ListTopics",
"sqs:ListQueues",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeInstanceInformation",
"ssm:DescribeMaintenanceWindows",
"ssm:DescribeMaintenanceWindowTargets",
"ssm:DescribeMaintenanceWindowTasks",
"ssm:DescribeParameters",
"ssm:DescribePatchBaselines",
"ssm-incidents:ListResponsePlans",
"ssm:ListAssociations",
"ssm:ListDocuments",
"ssm:ListInventoryEntries",
"ssm:ListResourceDataSync",
"states:ListActivities",
"states:ListStateMachines",
"timestream:ListDatabases",
"wisdom:listAssistantAssociations",
"wisdom:ListAssistants",
```

```
    "wisdom:listKnowledgeBases"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSResourceGroupsReadOnlyAccess

描述：这是 Res AWS ource Groups 的只读策略

AWSResourceGroupsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSResourceGroupsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 7 日 10:27 UTC
- 编辑时间：2019 年 2 月 5 日 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRoboMaker_FullAccess

描述：AWS RoboMaker 通过 AWS Management Console 和 SDK 提供对的完全访问权限。还提供对相关服务（例如 S3、IAM）的部分访问权限。

AWSRoboMaker_FullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSRoboMaker_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 10 日 18:34 UTC
- 编辑时间：2021 年 9 月 16 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
    }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRoboMakerReadOnlyAccess

描述：AWS RoboMaker 通过 AWS Management Console 和 SDK 提供只读访问权限

AWSRoboMakerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSRoboMakerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 26 日 05:30 UTC
- 编辑时间：2020 年 8 月 28 日 23:10 UTC

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

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRoboMakerServicePolicy

描述 : RoboMaker 服务策略

AWSRoboMakerServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 06:30 UTC
- 编辑时间：2021 年 11 月 11 日 22:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRoboMakerServiceRolePolicy

描述：RoboMaker 服务策略

AWSRoboMakerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSRoboMakerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 26 日 05:33 UTC
- 编辑时间：2018 年 11 月 26 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSRolesAnywhereServicePolicy

描述：允许 IAM Anywhere 角色代表您向私有证书颁发机构发布服务/使用情况指标 CloudWatch 并检查私有证书颁发机构的状况。

AWSRolesAnywhereServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 5 日 15:26 UTC
- 编辑时间：2022 年 7 月 5 日 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSS3OnOutpostsServiceRolePolicy

描述：允许 Outposts 上的 Amazon S3 服务代表你管理 EC2 网络资源。

AWSS3OnOutpostsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 10 月 3 日 20:32 UTC
- 编辑时间：2023 年 10 月 3 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSS3OutpostsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSavingsPlansFullAccess

描述：提供对 Savings Plans 服务的完全访问权限

AWSSavingsPlansFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSavingsPlansFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 6 日 22:45 UTC
- 编辑时间：2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : "savingsplans:*",
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSavingsPlansReadOnlyAccess

描述：提供对 Savings Plans 服务的只读访问权限

AWSSavingsPlansReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSavingsPlansReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 6 日 22:45 UTC
- 编辑时间：2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSecurityHubFullAccess

描述：提供使用 Security Hub 的完全访问权限。

AWSecurityHubFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSecurityHubFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 23:54 UTC

- 编辑时间：世界标准时间 2024 年 4 月 23 日 18:35
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    }
  ],
  {
    "Sid" : "OtherServicePermission",
    "Effect" : "Allow",
    "Action" : [
      "guardduty:GetDetector",
      "guardduty:ListDetectors",
      "inspector2:BatchGetAccountStatus",
      "pricing:GetProducts"
    ],
    "Resource" : "*"
  }
}
```

```
    }  
  ]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSecurityHubOrganizationsAccess

描述：授予在组织内启用和管理 Security Hub 的权限。包括在整个组织中启用该服务，以及确定该服务的委托管理员账户。

AWSecurityHubOrganizationsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSecurityHubOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 15 日 20:53 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 21:13
- ARN: arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSecurityHubReadOnlyAccess

描述：提供对 Sec AWS urity Hub 资源的只读访问权限

AWSecurityHubReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSecurityHubReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 01:34 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 23:45
- ARN: arn:aws:iam::aws:policy/AWSecurityHubReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSecurityHubServiceRolePolicy

描述：Sec AWS urity Hub 访问您的资源所需的服务相关角色。

AWSSecurityHubServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2018 年 11 月 27 日 23:47 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 03:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSecurityHubServiceRolePolicy

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogAdminFullAccess

描述：提供对服务目录管理功能的完全访问权限

AWSServiceCatalogAdminFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 15 日 17:19 UTC
- 编辑时间：2023 年 4 月 13 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogAdminReadOnlyAccess

描述：提供对 Service Catalog 管理功能的只读访问权限

AWSServiceCatalogAdminReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogAdminReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 25 日 18:53 UTC
- 编辑时间：2019 年 10 月 25 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogAppRegistryFullAccess

描述：提供对 Service Catalog 应用程序注册表功能的完全访问权限

AWSServiceCatalogAppRegistryFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogAppRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 12 日 22:25 UTC
- 编辑时间：世界标准时间 2023 年 12 月 7 日 21:50
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*"
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

描述：提供对 Service Catalog 应用程序注册表功能的只读访问权限

AWSServiceCatalogAppRegistryReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogAppRegistryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 12 日 22:34 UTC
- 编辑时间：2022 年 11 月 17 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

描述：允许 Service Catalog AppRegistry 代表你管理资源组

AWSServiceCatalogAppRegistryServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 18 日 22:18 UTC
- 编辑时间：2022 年 10 月 26 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogEndUserFullAccess

描述：提供对服务目录最终用户功能的完全访问权限

AWSServiceCatalogEndUserFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogEndUserFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 15 日 17:22 UTC
- 编辑时间：2019 年 7 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogEndUserReadOnlyAccess

描述：提供对 Service Catalog 最终用户功能的只读访问权限

AWSServiceCatalogEndUserReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSServiceCatalogEndUserReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 25 日 18:49 UTC
- 编辑时间：2019 年 10 月 25 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

描述：用于与 Organization AWS ServiceCatalog s AWS 组织结构同步的服务关联角色策略

AWSServiceCatalogOrgsDataSyncServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 10 日 20:48 UTC
- 编辑时间：2023 年 4 月 10 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceCatalogSyncServiceRolePolicy

描述：用于同步来自源存储库 AWS ServiceCatalog 的配置工件的服务关联角色

AWSServiceCatalogSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 15 日 21:20 UTC
- 编辑时间：世界标准时间 2024 年 5 月 3 日 17:12
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForAmazonEKSNodegroup

描述：管理客户账户中的节点组所需的权限。这些策略与以下资源的管理有关：AutoscalingGroups、SecurityGroups、LaunchTemplates 和 InstanceProfiles。

AWSServiceRoleForAmazonEKSNodegroup 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 7 日 01:34 UTC
- 编辑时间：世界标准时间 2024 年 1 月 4 日 20:37
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
],
"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"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iam:CreateInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:AddRoleToInstanceProfile"
  ],
  "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
},
{
  "Sid" : "PermissionsToManageEKSAndKubernetesTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "eks",
        "eks:cluster-name",
        "eks:nodegroup-name",
        "kubernetes.io/cluster/*"
      ]
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForAmazonQDeveloper

描述：此服务关联角色让 Amazon Q 开发人员能够提供使用信息。

AWSServiceRoleForAmazonQDeveloper 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 4 月 25 日 07:40
- 编辑时间：世界标准时间 2024 年 4 月 25 日 07:40
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

描述：提供对 CloudWatch 警报使用的 Systems Manager 资源的访问权限

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 10 月 1 日 09:49 UTC
- 编辑时间：2020 年 10 月 1 日 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Action" : [
      "ssm:CreateOpsItem"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

描述：CloudWatch 允许代表您访问 RDS Performance Insights 指标

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 9 月 7 日 09:32 UTC
- 编辑时间：2023 年 9 月 7 日 09:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForCodeGuru-Profiler

描述：Amazon CodeGuru Profiler 代表您发送通知所需的服务相关角色。

AWSServiceRoleForCodeGuru-Profiler 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 26 日 22:04 UTC
- 编辑时间：2020 年 6 月 26 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuruProfiler

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForCodeWhispererPolicy

描述：此角色授予访问您账户中数据 CodeWhisperer 以计算账单的权限，提供在 Amazon CodeGuru 中创建和访问安全报告以及向 CloudWatch 发送数据的权限。

AWSServiceRoleForCodeWhispererPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 24 日 19:39 UTC
- 编辑时间：世界标准时间 2024 年 3 月 29 日 22:13
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForEC2ScheduledInstances

描述：允许 EC2 计划实例启动和管理竞价型实例。

AWSServiceRoleForEC2ScheduledInstances 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 12 日 18:31 UTC
- 编辑时间：2017 年 10 月 12 日 18:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

描述：AWS GroundStation 使用此服务相关角色调用 EC2 来查找公有 IPv4 地址

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 12 月 13 日 23:52 UTC
- 编辑时间：2022 年 12 月 13 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForImageBuilder

描述：允许 EC2 ImageBuilder 代表您调用 AWS 服务。

AWSServiceRoleForImageBuilder 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 29 日 22:02 UTC
- 编辑时间：2023 年 10 月 19 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

策略版本

策略版本：v19 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForIoTSiteWise

描述： SiteWise 允许 AWS 物联网配置和管理网关以及查询数据。该策略包括部署到群组所需的 AWS Greengrass 权限、用于创建和更新服务前缀函数的 AWS Lambda 权限，以及用于从数据存储中查询数据的 IoT AWS Analytics 权限。

AWSServiceRoleForIoTSiteWise 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 14 日 19:19 UTC
- 编辑时间：2023 年 11 月 13 日 18:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
            "IOTSITWISE"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForLogDeliveryPolicy

描述：允许日志传送服务通过代表您调用日志目标来传送日志。

AWSServiceRoleForLogDeliveryPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 4 日 17:31 UTC
- 编辑时间：2021 年 7 月 15 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForMonitronPolicy

描述：授予 Amazon Monitron 管理 AWS 资源的权限，包括代表 AWS 您分配 SSO 用户。

AWSServiceRoleForMonitronPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 2 日 19:06 UTC
- 编辑时间：2022 年 9 月 29 日 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForNeptuneGraphPolicy

描述：提供 Cloudwatch 访问权限，用于发布亚马逊 Neptune 的运行和使用指标以及日志

AWSServiceRoleForNeptuneGraphPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 14:03
- 编辑时间：世界标准时间 2023 年 11 月 29 日 14:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

描述：提供描述和更新 Private Marketplace 资源以及描述 AWS Organisations 的权限

AWSServiceRoleForPrivateMarketplaceAdminPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 2 月 14 日 22:28
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:28

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForSMS

描述：提供访问服务实例所需的 AWS 服务和资源的访问权限，AWS 包括 EC2、S3 和 Cloudformation。

AWSServiceRoleForSMS是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 6 日 18:39 UTC
- 编辑时间：2020 年 10 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForUserSubscriptions

描述：提供对您的 Identity Center 资源的用户订阅服务的访问权限，以自动更新您的订阅。

AWSServiceRoleForUserSubscriptions 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 4 月 25 日 16:14
- 编辑时间：世界标准时间 2024 年 4 月 25 日 16:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRolePolicyForBackupReports

描述：提供 AWS Backup 权限以代表您创建合规报告

AWSServiceRolePolicyForBackupReports 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 19 日 21:16 UTC
- 编辑时间：2023 年 3 月 10 日 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRolePolicyForBackupRestoreTesting

描述：此策略包含测试恢复和清理测试期间创建的资源权限。

AWSServiceRolePolicyForBackupRestoreTesting 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 10 日 23:37 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:42
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSShieldDRTAccessPolicy

描述：在高严重性事件期间，为 AWS DDoS 响应团队提供有限的访问权限，AWS 账户 以协助缓解 DDoS 攻击。

AWSShieldDRTAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSShieldDRTAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 6 月 5 日 22:29 UTC
- 编辑时间：2020 年 12 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSShieldServiceRolePolicy

描述：允许 AWS Shield 代表您访问 AWS 资源以提供 DDoS 防护。

AWSShieldServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 17 日 19:17 UTC
- 编辑时间：2021 年 11 月 17 日 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Sid" : "AWSShield",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:GetWebACL",
    "wafv2:UpdateWebACL",
    "wafv2:GetWebACLForResource",
    "wafv2:ListResourcesForWebACL",
    "cloudfront:ListDistributions",
    "cloudfront:GetDistribution"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSMForSAPServiceLinkedRolePolicy

描述：为适用于 SAP 的 S AWS systems Manager 提供管理和集成 SAP 软件所需的权限 AWS。

AWSSSMForSAPServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 16 日 01:18 UTC
- 编辑时间：世界标准时间 2024 年 4 月 11 日 18:31
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "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:*: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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSMOpsInsightsServiceRolePolicy

描述：服务关联角色策略 AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 16 日 20:12 UTC
- 编辑时间：2021 年 6 月 16 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSODirectoryAdministrator

描述：SSO 目录的管理员访问权限

AWSSSODirectoryAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSSODirectoryAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 31 日 23:54 UTC
- 编辑时间：2022 年 10 月 20 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AWSSSODirectoryAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "sso-directory:*",
      "identitystore:*",
      "identitystore-auth:*",
      "sso:ListDirectoryAssociations"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSODirectoryReadOnly

描述：ReadOnly 访问 SSO 目录

AWSSSODirectoryReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSSSODirectoryReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 31 日 23:49 UTC
- 编辑时间：2022 年 11 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSOMasterAccountAdministrator

描述：在 AWS SSO 中提供访问权限以管理 Organizations 主账户和成员账户以及云应用程序

AWSSSOMasterAccountAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSSOMasterAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:36 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 00:38
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0CreateSLR",
      "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"
      }
    }
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSOMemberAccountAdministrator

描述：在 AWS SSO 中提供用于管理 Organization AWS s 成员账户和云应用程序的访问权限

AWSSSOMemberAccountAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSSOMemberAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:45 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 00:31
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSOReadOnly

描述：提供对 AWS SSO 配置的只读访问权限。

AWSSSOReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSSOReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:24 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 00:44
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

策略版本

策略版本 : v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSSOServiceRolePolicy

描述：授予 AWS SSO 权限以代表您管理 AWS 资源，包括 IAM 角色、策略和 SAML IdP。

AWSSSOServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 12 月 5 日 18:36 UTC
- 编辑时间：2022 年 10 月 20 日 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

策略版本

策略版本：v17 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStepFunctionsConsoleFullAccess

描述：一种访问策略，用于向用户/角色/等提供对控制台的访问权限。AWS StepFunctions 要获得完整的控制台体验，除了此策略外，用户可能还需要该服务可以担任的其他 IAM 角色的 iam: PassRole 权限。

AWSStepFunctionsConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSStepFunctionsConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:54 UTC
- 编辑时间：2017 年 1 月 12 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStepFunctionsFullAccess

描述：一种访问策略，用于向用户/角色/等提供对 API 的访问权限。AWS StepFunctions 要获得完全访问PassRole 权限，除此策略外，用户还必须对服务可以担任的至少一个 IAM 角色拥有 iam: 权限。

AWSStepFunctionsFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSStepFunctionsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:51 UTC
- 编辑时间：2017 年 1 月 11 日 21:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStepFunctionsReadOnlyAccess

描述：一种访问策略，用于为用户/角色/等提供对服务的只读访问权限。AWS StepFunctions

AWSStepFunctionsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSStepFunctionsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:46 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 18:53
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStorageGatewayFullAccess

描述：提供通过 AWS Storage Gateway 的完全访问权限 AWS Management Console。

AWSStorageGatewayFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSStorageGatewayFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2022 年 9 月 6 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStorageGatewayReadOnlyAccess

描述：提供通过 AWS Storage Gateway 的访问权限 AWS Management Console。

AWSStorageGatewayReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSStorageGatewayReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2022 年 9 月 6 日 20:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSStorageGatewayServiceRolePolicy

描述：Storage Gateway 使用的服务相关角色用于将其他 AWS 服务与 AWS Storage Gateway 集成。

AWSStorageGatewayServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 2 月 17 日 19:03 UTC
- 编辑时间：2021 年 2 月 17 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupplyChainFederationAdminAccess

描述： AWSSupplyChainFederationAdminAccess 为 AWS 供应链联合用户提供对 AWS 供应链应用程序的访问权限，包括在 AWS 供应链应用程序中执行操作所需的权限。该策略提供对 IAM Identity Center 用户和群组的管理权限，并附加到 Su AWS pply Chain 代表您创建的角色。您不应将 AWSSupplyChainFederationAdminAccess 策略附加到任何其他 IAM 实体。

AWSSupplyChainFederationAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupplyChainFederationAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 3 月 1 日 18:54 UTC
- 编辑时间：2023 年 11 月 1 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportAccess

描述：允许用户访问 AWS Support 中心。

AWSSupportAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : [
      "support:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportAppFullAccess

描述：提供对 AWS Support 应用程序和其他必需服务（例如 AWS Support 和 Service Quotas）的完全访问权限。此策略包括使用支持服务的权限，以使用户可以联系以 AWS Support 获取支持案例、更改服务配额以及创建相关的服务相关角色。

AWSSupportAppFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupportAppFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 22 日 16:53 UTC
- 编辑时间：2022 年 8 月 22 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportAppReadOnlyAccess

描述：提供对 AWS Support 应用程序的只读访问权限。

AWSSupportAppReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupportAppReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 22 日 17:01 UTC
- 编辑时间：2022 年 8 月 22 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportPlansFullAccess

描述：提供对支持计划的完全访问权限。

AWSSupportPlansFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupportPlansFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 27 日 18:19 UTC
- 编辑时间：2023 年 5 月 9 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "supportplans:GetSupportPlan",
      "supportplans:GetSupportPlanUpdateStatus",
      "supportplans:StartSupportPlanUpdate",
      "supportplans:CreateSupportPlanSchedule"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportPlansReadOnlyAccess

描述：提供对支持计划的只读访问权限。

AWSSupportPlansReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSupportPlansReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 27 日 18:08 UTC
- 编辑时间：2022 年 9 月 27 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSupportServiceRolePolicy

描述：允许 AWS Support 访问 AWS 资源以提供计费、管理和支持服务。

AWSSupportServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 4 月 19 日 18:04 UTC
- 编辑时间：世界标准时间 2024 年 5 月 2 日 02:47
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

策略版本

策略版本：v36 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AWSSupportActions",
  "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",
    "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",
"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",
"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:describeOperation",
"apprunner:describeService",
"apprunner:listAutoScalingConfigurations",
"apprunner:listConnections",
"apprunner:listOperations",
"apprunner:listServices",
"apprunner:listTagsForResource",
"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:getApiAssociation",
"appsync:getApiCache",
"appsync:getDomainName",
"appsync:getFunction",
"appsync:getGraphQLApi",
"appsync:getIntrospectionSchema",
"appsync:getResolver",
"appsync:getSchemaCreationStatus",
"appsync:getSourceApiAssociation",
"appsync:getType",
"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: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",
"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:describeWarmPool",
"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:listLegalHold",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup:listRestoreJobsByProtectedResource",
"backup:listRestoreTestingPlans",
"backup:listRestoreTestingSelections",
"backup:listTags",
"backup-gateway:getGateway",
"backup-gateway:getHypervisor",
"backup-gateway:getHypervisorPropertyMappings",
"backup-gateway:getVirtualMachine",
"backup-gateway:listGateways",
"backup-gateway:listHypervisors",
"backup-gateway:listVirtualMachines",
"batch:describeComputeEnvironments",
"batch:describeJobDefinitions",
"batch:describeJobQueues",
"batch:describeJobs",
"batch:listJobs",
"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: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",
"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: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",
"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:listWebhooks",
"codestar:describeProject",
"codestar:listProjects",
"codestar:listResources",
"codestar:listTeamMembers",
"codestar:listUserProfiles",
"codestar-connections:getConnection",
"codestar-connections:getHost",
"codestar-connections:listConnections",
"codestar-connections:listHosts",
"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:getECSServiceRecommendations",
"compute-optimizer:getECSServiceRecommendationProjectedMetrics",
"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",
"connect:describeContact",
"connect:describePhoneNumber",
"connect:describeQuickConnect",
"connect:describeUser",
"connect:getCurrentMetricData",
"connect:getMetricData",
"connect:listContactEvaluations",
"connect:listEvaluationForms",
"connect:listEvaluationFormVersions",
"connect:listPhoneNumbersV2",
"connect:listQuickConnects",
"connect:listRoutingProfiles",
"connect:listSecurityProfiles",
```

```
"connect:listUsers",
"connect:listViews",
"connect:listViewVersions",
"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:describeLocationEfs",
"datasync:describeLocationFsxLustre",
"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",
"dax:describeClusters",
"dax:describeDefaultParameters",
"dax:describeEvents",
"dax:describeParameterGroups",
"dax:describeParameters",
"dax:describeSubnetGroups",
"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",
"dml:getLifecyclePolicies",
"dml: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: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: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:describeInstanceCreditSpecifications",
"ec2:describeInstanceEventNotificationAttributes",
"ec2:describeInstanceEventWindows",
"ec2:describeInstances",
"ec2:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"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: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: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:describeTransitGateways",
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
```

```
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"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: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: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:describeImages",
"ecr:describeImageReplicationStatus",
"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:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"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:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"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: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:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"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",
"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",
"evidently:getExperiment",
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
```

```
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
"fms:listPolicies",
"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",
"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:getSession",
"glue:getStatement",
"glue:getTable",
"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: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:getDetector",
"guardduty:getFindings",
"guardduty:getFindingsStatistics",
"guardduty:getInvitationsCount",
"guardduty:getIPSet",
"guardduty:getMasterAccount",
"guardduty:getMembers",
"guardduty:getThreatIntelSet",
"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: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:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowBuildVersions",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflows",
"imagebuilder:listWorkflowStepExecutions",
"imagebuilder:listTagsForResource",
"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:getDelegatedAdminAccount",
"inspector2:getMember",
"inspector2:getSbomExport",
"inspector2:listCisScanConfigurations",
"inspector2:listCisScanResultsAggregatedByChecks",
"inspector2:listCisScanResultsAggregatedByTargetResource",
"inspector2:listCisScans",
"inspector2:listCoverage",
"inspector2:listDelegatedAdminAccounts",
"inspector2:listFilters",
"inspector2:listFindings",
"inspector2:listMembers",
"inspector2:listUsageTotals",
"inspector-scan:scanSbom",
"internetmonitor:getMonitor",
"internetmonitor:listMonitors",
"internetmonitor:getHealthEvent",
"internetmonitor:listHealthEvents",
"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: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:getFleet",
"iotfleetwise:getModelManifest",
"iotfleetwise:getSignalCatalog",
"iotfleetwise:getVehicle",
"iotfleetwise:getVehicleStatus",
"iotfleetwise:listCampaigns",
"iotfleetwise:listDecoderManifests",
"iotfleetwise:listDecoderManifestNetworkInterfaces",
"iotfleetwise:listDecoderManifestSignals",
"iotfleetwise:listFleets",
"iotfleetwise:listFleetsForVehicle",
"iotfleetwise:listModelManifests",
"iotfleetwise:listModelManifestNodes",
"iotfleetwise:listSignalCatalogs",
"iotfleetwise:listSignalCatalogNodes",
"iotfleetwise:listVehicles",
"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:getWorkspace",
"iottwinmaker:listComponentTypes",
"iottwinmaker:listEntities",
"iottwinmaker:listScenes",
"iottwinmaker:getSyncJob",
```

```
"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:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClientVpcConnections",
"kafka:listClusterOperations",
"kafka:listClusterOperationsV2",
"kafka:listClusters",
"kafka:listClustersV2",
"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:listStreams",
"kinesis:listStreamConsumers",
"kinesis:listTagsForStream",
"kinesisanalytics:describeApplication",
"kinesisanalytics:describeApplicationSnapshot",
"kinesisanalytics:listApplications",
"kinesisanalytics:listApplicationSnapshots",
"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: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:listVersionsByFunction",
"launchwizard:describeProvisionedApp",
"launchwizard:describeProvisioningEvents",
"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:describeLogGroups",
"logs:describeLogStreams",
"logs:describeMetricFilters",
"logs:describeQueries",
"logs:describeQueryDefinitions",
"logs:describeResourcePolicies",
"logs:describeSubscriptionFilters",
"logs:getDataProtectionPolicy",
"logs:getDelivery",
"logs:getDeliveryDestination",
"logs:getDeliveryDestinationPolicy",
"logs:getDeliverySource",
"logs:getLogAnomalyDetector",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listAnomalies",
"logs:listLogAnomalyDetectors",
"logs:listLogDeliveries",
"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",
"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:listChannels",
"medialive:listInputDevices",
"medialive:listInputs",
"medialive:listInputSecurityGroups",
"medialive:listMultiplexes",
"medialive:listOfferings",
"medialive:listReservations",
"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:getJourneyExecutionMetrics",
"mobiletargeting:getJourneyExecutionActivityMetrics",
"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",
"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",
"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",
"networkmanager:describeGlobalNetworks",
"networkmanager:getConnectAttachment",
"networkmanager:getConnections",
"networkmanager:getConnectPeer",
"networkmanager:getConnectPeerAssociations",
"networkmanager:getCoreNetwork",
"networkmanager:getCoreNetworkChangeEvents",
"networkmanager:getCoreNetworkChangeSet",
"networkmanager:getCoreNetworkPolicy",
"networkmanager:getCustomerGatewayAssociations",
"networkmanager:getDevices",
"networkmanager:getLinkAssociations",
"networkmanager:getLinks",
"networkmanager:getNetworkResourceCounts",
"networkmanager:getNetworkResourceRelationships",
"networkmanager:getNetworkResources",
"networkmanager:getNetworkRoutes",
"networkmanager:getNetworkTelemetry",
"networkmanager:getResourcePolicy",
"networkmanager:getRouteAnalysis",
"networkmanager:getSites",
"networkmanager:getSiteToSiteVpnAttachment",
"networkmanager:getTransitGatewayConnectPeerAssociations",
"networkmanager:getTransitGatewayPeering",
"networkmanager:getTransitGatewayRegistrations",
"networkmanager:getTransitGatewayRouteTableAttachment",
"networkmanager:getVpcAttachment",
"networkmanager:listAttachments",
"networkmanager:listConnectPeers",
"networkmanager:listCoreNetworkPolicyVersions",
"networkmanager:listCoreNetworks",
"networkmanager:listOrganizationServiceAccessStatus",
"networkmanager:listPeerings",
```

```
"networkmanager:listTagsForResource",
"networkmonitor:getMonitor",
"networkmonitor:getProbe",
"networkmonitor:listMonitors",
"nimble:getEula",
"nimble:getLaunchProfile",
"nimble:getLaunchProfileDetails",
"nimble:getLaunchProfileInitialization",
"nimble:getLaunchProfileMember",
"nimble:getStreamingImage",
"nimble:getStreamingSession",
"nimble:getStreamingSessionStream",
"nimble:getStudio",
"nimble:getStudioComponent",
"nimble:listEulaAcceptances",
"nimble:listEulas",
"nimble:listLaunchProfiles",
"nimble:listStreamingImages",
"nimble:listStreamingSessions",
"nimble:listStudioComponents",
"nimble:listStudios",
"notifications:getEventRule",
"notifications:getNotificationConfiguration",
"notifications:getNotificationEvent",
"notifications:listChannels",
"notifications:listEventRules",
"notifications:listNotificationConfigurations",
"notifications:listNotificationEvents",
"notifications:listNotificationHubs",
"notifications-contacts:getEmailContact",
"notifications-contacts:listEmailContacts",
"oam:getLink",
"oam:getSink",
"oam:getSinkPolicy",
"oam:listAttachedLinks",
"oam:listLinks",
"oam:listSinks",
"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:listReferenceStores",
"omics:listReferences",
"omics:listRunGroups",
"omics:listRunTasks",
"omics:listRuns",
"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:listAccounts",
"organizations:listTagsForResource",
"outposts:getCatalogItem",
"outposts:getConnection",
"outposts:getOrder",
"outposts:getOutpost",
"outposts:getOutpostInstanceTypes",
"outposts:getSite",
"outposts:listAssets",
"outposts:listCatalogItems",
"outposts:listOrders",
"outposts:listOutposts",
"outposts:listSites",
"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:listNetworks",
"private-networks:listNetworkResources",
"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:describeClusterParameterGroups",
"redshift:describeClusterParameters",
"redshift:describeClusters",
"redshift:describeClusterSecurityGroups",
"redshift:describeClusterSnapshots",
"redshift:describeClusterSubnetGroups",
"redshift:describeClusterVersions",
"redshift:describeDataShares",
"redshift:describeDataSharesForConsumer",
"redshift:describeDataSharesForProducer",
"redshift:describeDefaultClusterParameters",
"redshift:describeEventCategories",
"redshift:describeEvents",
"redshift:describeEventSubscriptions",
"redshift:describeHsmClientCertificates",
"redshift:describeHsmConfigurations",
"redshift:describeLoggingStatus",
"redshift:describeOrderableClusterOptions",
"redshift:describeReservedNodeOfferings",
"redshift:describeReservedNodes",
"redshift:describeResize",
"redshift:describeSnapshotCopyGrants",
"redshift:describeStorage",
"redshift:describeTableRestoreStatus",
"redshift:describeTags",
"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",
"rekognition:listCollections",
"rekognition:listFaces",
"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",
"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",
"rum:batchGetRumMetricDefinitions",
"rum:getAppMonitor",
"rum:listAppMonitors",
"rum:listRumMetricsDestinations",
"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:listMultipartUploadParts",
```

```
"s3:listMultiRegionAccessPoints",
"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: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: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:getEnabledStandards",
"securityhub:getFindings",
"securityhub:getInsightResults",
"securityhub:getInsights",
"securityhub:getMasterAccount",
"securityhub:getMembers",
"securityhub:listEnabledProductsForImport",
"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: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: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: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: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:listDocuments",
"ssm:listDocumentMetadataHistory",
"ssm:listDocumentVersions",
"ssm:listOpsItemEvents",
"ssm:listOpsItemRelatedItems",
"ssm:listOpsMetadata",
"ssm:listResourceComplianceSummaries",
```

```
"ssm:listResourceDataSync",
"ssm:listTagsForResource",
"sso:describeApplicationAssignment",
"sso:describeApplicationProvider",
"sso:describeApplication",
"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",
"tiros:createQuery",
"tiros:getQueryAnswer",
"tiros:getQueryExplanation",
"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:describeWorkflow",
"transfer:listAccesses",
"transfer:listAgreements",
"transfer:listConnectors",
"transfer:listExecutions",
"transfer:listHostKeys",
"transfer:listProfiles",
"transfer:listServers",
"transfer:listTagsForResource",
"transfer:listUsers",
"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: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:listServiceNetworks",
"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:describeIpGroups",
    "workspaces:describeTags",
    "workspaces:describeWorkspaceBundles",
    "workspaces:describeWorkspaceDirectories",
    "workspaces:describeWorkspaceImages",
    "workspaces:describeWorkspaces",
    "workspaces:describeWorkspacesConnectionStatus",
    "xray:getEncryptionConfig",
    "xray:getGroup",
    "xray:getGroups",
    "xray:getSamplingRules",
    "xray:listResourcePolicies"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
}
],
"Version" : "2012-10-17"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

描述：授予 S AWS systems Manager (SSM) 发现 AWS 账户 信息的权限。

AWSSystemsManagerAccountDiscoveryServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 24 日 17:21 UTC
- 编辑时间：2022 年 10 月 17 日 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSystemsManagerChangeManagementServicePolicy

描述：提供对 S AWS systems Manager 变更管理框架管理或使用的 AWS 资源的访问权限。

AWSSystemsManagerChangeManagementServicePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 7 日 22:21 UTC
- 编辑时间：2020 年 12 月 7 日 22:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSystemsManagerForSAPFullAccess

描述：提供对 SAP 服务的 S AWS systems Manager 的完全访问权限

AWSSystemsManagerForSAPFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSSystemsManagerForSAPFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2022 年 11 月 17 日 02:11 UTC
- 编辑时间：2022 年 11 月 18 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSystemsManagerForSAPReadOnlyAccess

描述：提供对 SAP 版 S AWS systems Manager 服务的只读访问权限

AWSSystemsManagerForSAPReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSSystemsManagerForSAPReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 17 日 02:11 UTC
- 编辑时间：2022 年 11 月 17 日 02:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:get*",
      "ssm-sap:list*"
    ],
    "Resource" : "arn:*:ssm-sap:*:*:*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

描述：SSM 资源管理器的 IAM 角色，用于管理 OpsData 相关操作

AWSSystemsManagerOpsDataSyncServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 26 日 20:42 UTC
- 编辑时间：2023 年 6 月 28 日 22:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxAssetServerPolicy

描述：此策略向 AWS 门户资产服务器授予正常操作所需的必要权限。

AWSThinkboxAssetServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxAssetServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:18 UTC
- 编辑时间：2020 年 5 月 27 日 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxAWSPortalAdminPolicy

描述：该政策授予 AWS Thinkbox 的 Deadline 软件对 AWS 门户管理所需的多项 AWS 服务的完全访问权限。这包括对多种 EC2 资源类型创建任意标签的权限。

AWSThinkboxAWSPortalAdminPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxAWSPortalAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:41 UTC
- 编辑时间：世界标准时间 2024 年 4 月 12 日 20:07
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
    "StringLike" : {
      "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" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal6",
  "Effect" : "Allow",
```

```
"Action" : "ec2:TerminateInstances",
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
  }
}
},
{
  "Sid" : "AWSThinkboxAWSPortal7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:PlacementGroup" : "*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:rsc-tls-pw*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxAWSPortalGatewayPolicy

描述：此策略向 AWS 门户网关计算机授予正常操作所需的必要权限。

AWSThinkboxAWSPortalGatewayPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxAWSPortalGatewayPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:05 UTC
- 编辑时间：2020 年 6 月 30 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:rds-tls-pw-stack*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxAWSPortalWorkerPolicy

描述：此策略向 AWS 门户网站中的截止日期工作人员授予正常操作所需的必要权限。

AWSThinkboxAWSPortalWorkerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxAWSPortalWorkerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:15 UTC
- 编辑时间：2020 年 12 月 7 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

描述：授予运行 AWS Thinkbox 的截止日期资源跟踪器所需的权限。这包括对某些 EC2 操作的完全访问权限，包括 DeleteFleets 和 CancelSpotFleetRequests。

AWSThinkboxDeadlineResourceTrackerAccessPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxDeadlineResourceTrackerAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:25 UTC
- 编辑时间：2020 年 5 月 27 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineResourceTrackerAccessPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

描述：授予创建、销毁和管理 AWS Thinkbox 的截止日期资源跟踪器所需的权限。

AWSThinkboxDeadlineResourceTrackerAdminPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSThinkboxDeadlineResourceTrackerAdminPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:29 UTC
- 编辑时间：世界标准时间 2024 年 4 月 12 日 20:55
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : {
      "StringLike" : {
        "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*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

描述：授予 AWS Thinkbox 的 Deadline Spot 活动插件所需的权限。这包括请求、修改和取消竞价队列的权限以及有限的 PassRole 权限。

AWSThinkboxDeadlineSpotEventPluginAdminPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxDeadlineSpotEventPluginAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:38 UTC
- 编辑时间：2020 年 5 月 27 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginAdminPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

描述：授予运行 AWS Thinkbox Deadline Spot 事件插件工作程序软件的 EC2 实例所需的权限。

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:35 UTC
- 编辑时间：2020 年 12 月 7 日 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTransferConsoleFullAccess

描述：提供通过 Transfer AWS 的完全访问权限 AWS Management Console

AWSTransferConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSTransferConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 14 日 19:33 UTC
- 编辑时间：2020 年 12 月 14 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTransferFullAccess

描述：提供对 AWS 传输服务的完全访问权限。

AWSTransferFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSTransferFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 14 日 19:37 UTC
- 编辑时间：2020 年 12 月 14 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTransferLoggingAccess

描述：允许 AWS 转移完全访问权限以创建日志流和群组并将日志事件存入您的账户

AWSTransferLoggingAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSTransferLoggingAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 14 日 15:32 UTC

- 编辑时间：2019 年 1 月 14 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTransferReadOnlyAccess

描述：提供对 AWS 传输服务的只读访问权限。

AWSTransferReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSTransferReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 27 日 17:54 UTC
- 编辑时间：2020 年 8 月 27 日 17:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTrustedAdvisorPriorityFullAccess

描述：提供对 T AWS rusted Advisor Priority 的完全访问权限。此策略还允许用户将 Trusted Advisor 作为可信服务添加到 AWS 组织，并为 Trusted Advisor Priority 指定委托管理员帐户。

AWSTrustedAdvisorPriorityFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSTrustedAdvisorPriorityFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 16 日 16:08 UTC
- 编辑时间：2022 年 8 月 16 日 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

描述：提供对 T AWS rusted Advisor 优先级的只读访问权限。这包括查看委派管理员账户的权限。

AWSTrustedAdvisorPriorityReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSTrustedAdvisorPriorityReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 16 日 16:35 UTC
- 编辑时间：2022 年 8 月 16 日 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTrustedAdvisorReportingServiceRolePolicy

描述：Trusted Advisor 多账户报告的服务政策

AWSTrustedAdvisorReportingServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 19 日 17:41 UTC
- 编辑时间：2023 年 2 月 28 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSTrustedAdvisorServiceRolePolicy

描述：访问 T AWS rusted Advisor 服务，以帮助降低成本、提高性能和提高 AWS 环境安全性。

AWSTrustedAdvisorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 2 月 22 日 21:24 UTC
- 编辑时间：世界标准时间 2024 年 6 月 11 日 18:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSUserNotificationsServiceLinkedRolePolicy

描述：允许 AWS 用户通知代表您呼叫 AWS 服务。

AWSUserNotificationsServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- **类型：**服务相关角色策略
- **创建时间：**2023 年 4 月 19 日 13:28 UTC
- **编辑时间：**2023 年 4 月 19 日 13:28 UTC
- **ARN:** arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVendorInsightsAssessorFullAccess

描述：提供查看名为“供应商见解”资源和管理供应商见解订阅的完全访问权限

AWSVendorInsightsAssessorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSVendorInsightsAssessorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVendorInsightsAssessorReadOnly

描述：提供只读访问权限，用于查看名为“供应商见解”的资源

AWSVendorInsightsAssessorReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSVendorInsightsAssessorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVendorInsightsVendorFullAccess

描述：为创建和管理供应商见解资源提供完全访问权限

AWSVendorInsightsVendorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSVendorInsightsVendorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2023 年 10 月 19 日 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVendorInsightsVendorReadOnly

描述：提供只读访问权限，用于查看供应商见解资源

AWSVendorInsightsVendorReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSVendorInsightsVendorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVpcLatticeServiceRolePolicy

描述：允许 VPC Lattice 代表您访问 AWS 资源。

AWSVpcLatticeServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2022 年 11 月 30 日 20:47 UTC
- 编辑时间：2022 年 11 月 30 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVPCS2SVpnServiceRolePolicy

描述：允许站点到站点 VPN 创建和管理与您的 VPN 连接相关的资源。

AWSVPCS2SVpnServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 6 日 14:13 UTC
- 编辑时间：2019 年 8 月 6 日 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```


了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVPCTransitGatewayServiceRolePolicy

描述：允许 VPC Transit Gateway 为你的 Transit Gateway VPC 附件创建和管理必要的资源。

AWSVPCTransitGatewayServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 16:21 UTC
- 编辑时间：2021 年 4 月 15 日 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSVPCVerifiedAccessServiceRolePolicy

描述：允许 AWS 验证访问服务以代表您配置终端节点的策略

AWSVPCVerifiedAccessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 29 日 03:35 UTC
- 编辑时间：世界标准时间 2023 年 11 月 17 日 21:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWAFConsoleFullAccess

描述：通过提供对 AWS WAF 的完全访问权限。AWS Management Console 请注意，该政策还授予列出和更新亚马逊 CloudFront 分配的权限、在 AWS Elastic Load Balancing 上查看负载均衡器的权限、

查看 Amazon API Gateway REST API 和阶段的权限、列出和查看亚马逊 CloudWatch 指标的权限以及查看账户内启用的区域的权限。

AWSWAFConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSWAFConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 6 日 18:38 UTC
- 编辑时间：2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:SetWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",

```

```

    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:SetWebACL",
    "appsync:ListGraphQLApis",
    "appsync:SetWebACL",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "s3:ListAllMyBuckets",
    "logs:DescribeResourcePolicies",
    "logs:DescribeLogGroups",
    "cognito-idp:ListUserPools",
    "cognito-idp:AssociateWebACL",
    "cognito-idp:DisassociateWebACL",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-idp:GetWebACLForResource",
    "apprunner:AssociateWebAcl",
    "apprunner:DisassociateWebAcl",
    "apprunner:DescribeWebAclForService",
    "apprunner:ListServices",
    "apprunner:ListAssociatedServicesForWebAcl",
    "ec2:AssociateVerifiedAccessInstanceWebAcl",
    "ec2:DisassociateVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
    "ec2:GetVerifiedAccessInstanceWebAcl",
    "ec2:DescribeVerifiedAccessInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowLogDeliverySubscription",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs>DeleteLogDelivery"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
  "Action" : [
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
  ],
  "Resource" : [

```

```
    "arn:aws:s3:::aws-waf-logs-*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
  "Action" : [
    "logs:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Effect" : "Allow",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "wafv2.amazonaws.com"
      ]
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWAFConsoleReadOnlyAccess

描述：通过提供对 AWS WAF 的只读访问权限。AWS Management Console 请注意，该政策还授予列出亚马逊 CloudFront 分配的权限、在 AWS Elastic Load Balancing 上查看负载均衡器的权限、查看 Amazon API Gateway REST API 和阶段的权限、列出和查看亚马逊 CloudWatch 指标的权限以及查看账户内启用的区域的权限。

AWSWAFConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSWAFConsoleReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 6 日 18:43 UTC
- 编辑时间：2023 年 6 月 5 日 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "apigateway:GET",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "appsync:ListGraphQLApis",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:Describe*",
        "wafv2:Get*",

```



```
"wafv2:List*",
"wafv2:CheckCapacity",
"cognito-idp:ListUserPools",
"cognito-idp:ListResourcesForWebACL",
"cognito-idp:GetWebACLForResource",
"apprunner:DescribeWebAclForService",
"apprunner:ListServices",
"apprunner:ListAssociatedServicesForWebAcl",
"ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
"ec2:GetVerifiedAccessInstanceWebAcl",
"ec2:DescribeVerifiedAccessInstances"
],
"Effect" : "Allow",
"Resource" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWAFFullAccess

描述：提供对 AWS WAF 操作的完全访问权限。

AWSWAFFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSWAFFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 6 日 20:44 UTC

- 编辑时间：2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*",
        "wafv2:*",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "appsync:SetWebACL",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWAFReadOnlyAccess

描述：提供对 AWS WAF 操作的只读访问权限。

AWSWAFReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSWAFReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 6 日 20:43 UTC
- 编辑时间：2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",

```

```
    "wafv2:Get*",
    "wafv2:List*",
    "wafv2:Describe*",
    "wafv2:CheckCapacity",
    "cognito-idp:ListResourcesForWebACL",
    "cognito-idp:GetWebACLForResource",
    "apprunner:DescribeWebAclForService",
    "apprunner:ListServices",
    "apprunner:ListAssociatedServicesForWebAcl",
    "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
    "ec2:GetVerifiedAccessInstanceWebAcl"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

描述：WellArchitected 允许代表客户访问与 WellArchitected 资源相关的 AWS 服务和资源。

AWSWellArchitectedDiscoveryServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 26 日 18:36 UTC

- 编辑时间：2023 年 4 月 26 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
```

```
    "servicelog:ListAssociatedResources",
    "servicelog:GetApplication",
    "servicelog>CreateAttributeGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicelog:AssociateAttributeGroup",
    "servicelog:DisassociateAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicelog:*:*:/applications/*",
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicelog:UpdateAttributeGroup",
    "servicelog>DeleteAttributeGroup"
  ],
  "Resource" : [
    "arn:*:servicelog:*:*:/attribute-groups/AWS_WellArchitected-*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

描述：允许 Well-Architected 代表你访问组织。

AWSWellArchitectedOrganizationsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 6 月 23 日 17:15 UTC
- 编辑时间：2022 年 7 月 25 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```



```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSWickrFullAccess

描述：此策略向 Wickr 服务授予完全管理权限，包括下的 Wickr 管理功能。AWS Management Console

AWSWickrFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSWickrFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 20:36 UTC
- 编辑时间：2022 年 11 月 27 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [  
  {  
    "Effect" : "Allow",  
    "Action" : "wickr:*",  
    "Resource" : "*"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayCrossAccountSharingConfiguration

描述：提供管理 Observability Access Manager 链接和建立 X-Ray 轨迹共享的功能

AWSXrayCrossAccountSharingConfiguration是一个[AWS 托管策略](#)。

使用此策略

您可以将 AWSXrayCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:46 UTC
- 编辑时间：2022 年 11 月 27 日 13:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXRayDaemonWriteAccess

描述：允许 AWS X-Ray Daemon 将原始跟踪段数据中继到服务的 API，并检索要由 X-Ray SDK 使用的采样数据（规则、目标等）。

AWSXRayDaemonWriteAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSXRayDaemonWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 8 月 28 日 23:00 UTC
- 编辑时间：世界标准时间 2024 年 2 月 13 日 21:58
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayFullAccess

描述：AWS X-Ray 完全访问托管策略

AWSXrayFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSXrayFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:30 UTC
- 编辑时间：世界标准时间 2024 年 4 月 11 日 17:07
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayReadOnlyAccess

描述：AWS X-Ray 只读托管策略

AWSXrayReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `AWSXrayReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:27 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 00:35
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayWriteOnlyAccess

描述：AWS X-Ray 仅写入托管策略

AWSXrayWriteOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 AWSXrayWriteOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:19 UTC
- 编辑时间：2018 年 8 月 28 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

描述：为 ARC 分区轮班练习提供管理访问权限，以及访问 CloudWatch 警报状态以监控练习跑步。

AWSZonalAutoshiftPracticeRunSLRPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 17:34
- 编辑时间：世界标准时间 2023 年 11 月 29 日 17:34
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

BatchServiceRolePolicy

描述：为 Batch AWS 服务提供管理所需资源的访问权限，包括 Amazon EC2 和 Amazon ECS 资源。

BatchServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 3 月 10 日 06:55 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 22:52
- ARN: arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Billing

描述：授予账单和成本管理权限。这包括查看账户使用量，以及查看和修改预算和付款方式。

Billing是一个[AWS 托管策略](#)。

使用此策略

您可以将 Billing 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:33 UTC
- 编辑时间：世界标准时间 2024 年 5 月 23 日 23:26
- ARN: arn:aws:iam::aws:policy/job-function/Billing

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
```

```
"Effect" : "Allow",
"Action" : [
  "account:GetAccountInformation",
  "aws-portal:*Billing",
  "aws-portal:*PaymentMethods",
  "aws-portal:*Usage",
  "billing:GetBillingData",
  "billing:GetBillingDetails",
  "billing:GetBillingNotifications",
  "billing:GetBillingPreferences",
  "billing:GetContractInformation",
  "billing:GetCredits",
  "billing:GetIAMAccessPreference",
  "billing:GetSellerOfRecord",
  "billing:ListBillingViews",
  "billing:PutContractInformation",
  "billing:RedeemCredits",
  "billing:UpdateBillingPreferences",
  "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:GetInvoiceEmailDeliveryPreferences",
" invoicing:GetInvoicePDF",
" invoicing:ListInvoiceSummaries",
" invoicing:PutInvoiceEmailDeliveryPreferences",
" payments:CreatePaymentInstrument",
" payments>DeletePaymentInstrument",
" payments:GetPaymentInstrument",
" payments:GetPaymentStatus",
" payments:ListPaymentPreferences",
" payments:ListTagsForResource",
" payments:ListPaymentInstruments",
" payments:MakePayment",
" payments:TagResource",
" payments:UpdatePaymentPreferences",
" payments:UpdatePaymentInstrument",
" payments:UntagResource",
" 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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CertificateManagerServiceRolePolicy

描述：Amazon Certificate Manager 服务角色政策

CertificateManagerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 25 日 17:56 UTC
- 编辑时间：2020 年 6 月 25 日 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

ClientVPNServiceConnectionsRolePolicy

描述：允许 AWS Client VPN 管理您的客户端 VPN 端点连接的策略。

ClientVPNServiceConnectionsRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 12 日 19:48 UTC
- 编辑时间：2020 年 8 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
```

```
    }  
  ]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ClientVPNServiceRolePolicy

描述：允许 AWS 客户端 VPN 管理您的客户端 VPN 端点的策略。

ClientVPNServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 12 月 10 日 21:20 UTC
- 编辑时间：2020 年 8 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

描述：CloudFormation StackSets（组织主账户）的服务角色

CloudFormationStackSetsOrgAdminServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 10 日 00:20 UTC
- 编辑时间：2019 年 12 月 10 日 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

描述：CloudFormation StackSets（组织成员账户）的服务角色

CloudFormationStackSetsOrgMemberServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 9 日 23:52 UTC
- 编辑时间：2019 年 12 月 9 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudFrontFullAccess

描述：提供对 CloudFront 控制台的完全访问权限以及通过列出 Amazon S3 存储桶的 AWS Management Console 功能。

CloudFrontFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudFrontFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：世界标准时间 2024 年 1 月 4 日 16:56
- ARN: arn:aws:iam::aws:policy/CloudFrontFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cfffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ]
    }
  ]
}
```

```
    "wafv2:ListWebACLs",
    "wafv2:GetWebACL",
    "kinesis:ListStreams"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "cffdescribestream",
  "Action" : [
    "kinesis:DescribeStream"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:kinesis:*:*:*"
},
{
  "Sid" : "cfflistroles",
  "Action" : [
    "iam:ListRoles"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam:*:*:*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudFrontReadOnlyAccess

描述：允许通过访问 CloudFront 分发配置信息和列表分发 AWS Management Console。

CloudFrontReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudFrontReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：世界标准时间 2024 年 1 月 4 日 16:55
- ARN: arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudHSMServiceRolePolicy

描述：允许访问 CloudHSM 使用或管理的 AWS 资源

CloudHSMServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 6 日 19:12 UTC
- 编辑时间：2017 年 11 月 6 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudSearchFullAccess

描述：提供对 Amazon CloudSearch 配置服务的完全访问权限。

CloudSearchFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudSearchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC

- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudSearchReadOnlyAccess

描述：提供对 Amazon CloudSearch 配置服务的只读访问权限。

CloudSearchReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudSearchReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudTrailServiceRolePolicy

描述：的权限策略 CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 10 月 24 日 21:21 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 01:18
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatch-CrossAccountAccess

描述：CloudWatch 允许代表当前账户在远程账户中 CrossAccountSharing 扮演角色，以便跨账户、跨区域显示数据 CloudWatch

CloudWatch-CrossAccountAccess 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 7 月 23 日 09:59 UTC
- 编辑时间：2019 年 7 月 23 日 09:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchActionsEC2Access

描述：提供对 CloudWatch 警报和指标以及 EC2 元数据的只读访问权限。提供停止、终止和重启 EC2 实例的访问权限。

CloudWatchActionsEC2Access 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchActionsEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 7 月 7 日 00:00 UTC
- 编辑时间：2015 年 7 月 7 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchAgentAdminPolicy

描述：需要完全权限才能使用 AmazonCloudWatchAgent。

CloudWatchAgentAdminPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchAgentAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 7 日 00:52 UTC
- 编辑时间：世界标准时间 2024 年 2 月 5 日 20:59
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchAgentServerPolicy

描述：AmazonCloudWatchAgent 在服务器上使用所需的权限

CloudWatchAgentServerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchAgentServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 7 日 01:06 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 16:37
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchApplicationInsightsFullAccess

描述：提供对“CloudWatch 应用程序见解”和所需依赖项的完全访问权限。

CloudWatchApplicationInsightsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchApplicationInsightsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 24 日 18:44 UTC
- 编辑时间：2022 年 1 月 25 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchApplicationInsightsReadOnlyAccess

描述：提供对“CloudWatch 应用程序见解”的只读访问权限。

CloudWatchApplicationInsightsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchApplicationInsightsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 24 日 18:48 UTC

- 编辑时间：2020 年 11 月 24 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

描述：Cloudwatch 应用程序洞察服务关联角色策略

CloudwatchApplicationInsightsServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 12 月 1 日 16:22 UTC
- 编辑时间：2023 年 5 月 11 日 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

策略版本

策略版本：v24（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch>DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents",
      "logs:GetLogEvents",
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudFormation:CreateStack",
      "cloudFormation:UpdateStack",
      "cloudFormation>DeleteStack",
      "cloudFormation:DescribeStackResources"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudFormation:DescribeStacks",
      "cloudFormation:ListStackResources",
      "cloudFormation:ListStacks"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups>DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "autoscaling:DescribeAutoScalingGroups"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter",
      "ssm>DeleteParameter",
      "ssm:AddTagsToResource",
      "ssm:RemoveTagsFromResource",
      "ssm:GetParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
  },
  {
    "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"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetOpsItem",
      "ssm:CreateOpsItem",
      "ssm:DescribeOpsItems",
      "ssm:UpdateOpsItem",
      "ssm:DescribeInstanceInformation"
    ]
  }

```

```
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:AddTagsToResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:opsitem/*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "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"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
    ],
    "Resource" : [
```

```
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions",
    "lambda:GetFunctionConfiguration",
    "lambda:ListEventSourceMappings"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "xray:GetServiceGraph",
    "xray:GetTraceSummaries",
    "xray:GetTimeSeriesServiceStatistics",
    "xray:GetTraceGraph"
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:ListTables",
      "dynamodb:DescribeTable",
      "dynamodb:DescribeContributorInsights",
      "dynamodb:DescribeTimeToLive"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DescribeScalableTargets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets",
      "s3:GetMetricsConfiguration",
      "s3:GetReplicationConfiguration"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "states:ListStateMachines",
      "states:DescribeExecution",
      "states:DescribeStateMachine",
      "states:GetExecutionHistory"
    ],
  },
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeClusters",
      "ecs:DescribeContainerInstances",
      "ecs:DescribeServices",
      "ecs:DescribeTaskDefinition",
      "ecs:DescribeTasks",
      "ecs:DescribeTaskSets",
      "ecs:ListClusters",
      "ecs:ListContainerInstances",
      "ecs:ListServices",
      "ecs:ListTasks"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:UpdateClusterSettings"
    ],
    "Resource" : [
      "arn:aws:ecs:*:*:cluster/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "eks:DescribeCluster",
```

```
    "eks:DescribeFargateProfile",
    "eks:DescribeNodegroup",
    "eks:ListClusters",
    "eks:ListFargateProfiles",
    "eks:ListNodegroups",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:GetSubscriptionAttributes",
    "sns:GetTopicAttributes",
    "sns:GetSMSAttributes",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs>DeleteSubscriptionFilter"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
```



```
    "logs:PutSubscriptionFilter"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*",
    "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFileSystems"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53:GetHostedZone",
    "route53:GetHealthCheck",
    "route53>ListHostedZones",
    "route53>ListHealthChecks",
    "route53>ListQueryLoggingConfigs"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:ListFirewallRuleGroupAssociations",
    "route53resolver:GetFirewallRuleGroup",
    "route53resolver>ListFirewallRuleGroups",
    "route53resolver>ListResolverEndpoints",
    "route53resolver:GetResolverQueryLogConfig",
    "route53resolver>ListResolverQueryLogConfigs",
    "route53resolver>ListResolverQueryLogConfigAssociations",
    "route53resolver:GetResolverEndpoint",
    "route53resolver:GetFirewallRuleGroupAssociation"
  ],
  "Resource" : [
```

```
        "*"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchApplicationSignalsFullAccess

描述：提供对 App CloudWatch lication Signals 服务的完全访问权限，以及对使用和操作此服务所需的依赖项的限定访问权限。

CloudWatchApplicationSignalsFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchApplicationSignalsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 6 月 6 日 22:50
- 编辑时间：世界标准时间 2024 年 6 月 6 日 22:50
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchApplicationSignalsReadOnlyAccess

描述：提供对 App CloudWatch lication Signals 服务的只读访问权限以及对使用此服务所需的依赖项的限定访问权限

CloudWatchApplicationSignalsReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchApplicationSignalsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 6 月 6 日 22:48
- 编辑时间：世界标准时间 2024 年 6 月 6 日 22:48
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchApplicationSignalsServiceRolePolicy

描述：策略授予 CloudWatch 应用程序信号从其他相关 AWS 服务收集监控和标记数据的权限。

CloudWatchApplicationSignalsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 9 日 18:09 UTC
- 编辑时间：世界标准时间 2024 年 4 月 26 日 21:29
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "EC2AutoScalingPermission",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAutoScalingGroups"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchAutomaticDashboardsAccess

描述：提供对用于显示 CloudWatch 自动仪表板的非 CloudWatch API 的访问权限，包括 Lambda 函数等对象的内容

CloudWatchAutomaticDashboardsAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchAutomaticDashboardsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 23 日 10:01 UTC
- 编辑时间：2021 年 4 月 20 日 13:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchCrossAccountSharingConfiguration

描述：提供管理可观测性访问管理器链接和建立资源共享的 CloudWatch 功能

CloudWatchCrossAccountSharingConfiguration 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 14:01 UTC
- 编辑时间：2022 年 11 月 27 日 14:01 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchEventsBuiltInTargetExecutionAccess

描述：允许 Amazon Ev CloudWatch ents 中的内置目标代表您执行 EC2 操作。

CloudWatchEventsBuiltInTargetExecutionAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchEventsBuiltInTargetExecutionAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 14 日 18:35 UTC
- 编辑时间：2016 年 1 月 14 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```


了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchEventsFullAccess

描述：提供对 Amazon CloudWatch 活动的完全访问权限。

CloudWatchEventsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchEventsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 14 日 18:37 UTC
- 编辑时间：2022 年 12 月 1 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
    "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchEventsInvocationAccess

描述：允许 Amazon E CloudWatch vents 将事件中继到您账户中 AWS Kinesis Streams 中的直播中。

CloudWatchEventsInvocationAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchEventsInvocationAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 14 日 18:36 UTC
- 编辑时间：2016 年 1 月 14 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchEventsReadOnlyAccess

描述：提供对 Amazon CloudWatch 活动的只读访问权限。

CloudWatchEventsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchEventsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 14 日 18:27 UTC
- 编辑时间：2022 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"}
```

```
    }  
  ]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchEventsServiceRolePolicy

描述：AWS CloudWatch 允许代表您执行通过警报和事件配置的操作。

CloudWatchEventsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 17 日 00:42 UTC
- 编辑时间：2017 年 11 月 17 日 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchFullAccess

描述：提供对的完全访问权限 CloudWatch。

CloudWatchFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2022 年 11 月 27 日 13:23 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchFullAccessV2

描述：提供对的完全访问权限 CloudWatch。

CloudWatchFullAccessV2是一个[AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchFullAccessV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 1 日 11:32 UTC
- 编辑时间：世界标准时间 2024 年 5 月 17 日 22:20
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchInternetMonitorServiceRolePolicy

描述：允许 Internet Monitor 代表您访问 EC2、工作空间、CloudFront 资源以及其他必需的服务。

CloudWatchInternetMonitorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 27 日 17:46 UTC
- 编辑时间：2023 年 7 月 20 日 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchLambdaInsightsExecutionRolePolicy

描述：Lambda Insights 扩展程序所需的策略

CloudWatchLambdaInsightsExecutionRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchLambdaInsightsExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2020 年 10 月 7 日 19:27 UTC
- 编辑时间：2020 年 10 月 7 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchLogsCrossAccountSharingConfiguration

描述：提供管理 Observability Access Manager 链接和建立 CloudWatch 日志资源共享的功能

CloudWatchLogsCrossAccountSharingConfiguration 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchLogsCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:55 UTC
- 编辑时间：2022 年 11 月 27 日 13:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchLogsFullAccess

描述：提供对 CloudWatch 日志的完全访问权限

CloudWatchLogsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchLogsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 18:12
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchLogsReadOnlyAccess

描述：提供对 CloudWatch 日志的只读访问权限

CloudWatchLogsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchLogsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 18:11
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchNetworkMonitorServiceRolePolicy

描述：允许 CloudWatch Network Monitor 访问和管理 EC2 和 VPC 资源、发布数据 CloudWatch 并代表您访问其他必需的服务。

CloudWatchNetworkMonitorServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 12 月 21 日 18:53
- 编辑时间：世界标准时间 2023 年 12 月 21 日 18:53
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchReadOnlyAccess

描述：提供对的只读访问权限 CloudWatch。

CloudWatchReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 5 月 17 日 22:17
- ARN: arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
      ],
    },
  ],
}
```

```
    "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"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchSyntheticsFullAccess

描述：提供对 S CloudWatch synthetics 的完全访问权限。

CloudWatchSyntheticsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchSyntheticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2019 年 11 月 25 日 17:39 UTC
- 编辑时间 : 2022 年 5 月 6 日 18:14 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

策略版本

策略版本 : v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "lambda:CreateFunction",
    "lambda:AddPermission",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration",
    "lambda:GetFunctionConfiguration",
```

```
    "lambda:DeleteFunction"
  ],
  "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:*"
  ]
},
{
  "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"
            ]
        }
    }
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchSyntheticsReadOnlyAccess

描述：提供对 Synthetics 的只读 CloudWatch 访问权限。

CloudWatchSyntheticsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CloudWatchSyntheticsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 25 日 17:45 UTC
- 编辑时间：2020 年 3 月 6 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComprehendDataAccessRolePolicy

描述：AWS Comprehend 服务角色的策略，该策略允许访问 S3 资源以进行数据访问

ComprehendDataAccessRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ComprehendDataAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 3 月 6 日 22:28 UTC
- 编辑时间：2019 年 3 月 6 日 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : {
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*Comprehend*",
    "arn:aws:s3:::*comprehend*"
  ]
}
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComprehendFullAccess

描述：提供对亚马逊 Comprehend 的完全访问权限。

ComprehendFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ComprehendFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 18:08 UTC
- 编辑时间：2017 年 12 月 5 日 01:36 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComprehendMedicalFullAccess

描述：提供对亚马逊 Comprehend Medical 的完全访问权限

ComprehendMedicalFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `ComprehendMedicalFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 17:55 UTC
- 编辑时间：2018 年 11 月 27 日 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComprehendReadOnly

描述：提供对 Amazon Comprehend 的只读访问权限。

ComprehendReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ComprehendReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 18:10 UTC
- 编辑时间：2022 年 4 月 26 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendReadOnly

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComputeOptimizerReadOnlyAccess

描述：提供对的只读访问权限 ComputeOptimizer。

ComputeOptimizerReadOnlyAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 ComputeOptimizerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 3 月 7 日 00:11 UTC
- 编辑时间：2023 年 8 月 28 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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:GetLicenseRecommendations",
"ec2:DescribeInstances",
"ec2:DescribeVolumes",
"ecs:ListServices",
"ecs:ListClusters",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeAutoScalingInstances",
"lambda:ListFunctions",
"lambda:ListProvisionedConcurrencyConfigs",
"cloudwatch:GetMetricData",
"organizations:ListAccounts",
"organizations:DescribeOrganization",
"organizations:DescribeAccount"
  ],
  "Resource" : "*"
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ComputeOptimizerServiceRolePolicy

描述：ComputeOptimizer 允许代表您呼叫 AWS 服务并收集工作量详细信息。

ComputeOptimizerServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 08:45 UTC
- 编辑时间：2022 年 6 月 13 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScalingAccess",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeAutoScalingGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2Access",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ConfigConformsServiceRolePolicy

描述：创建一致性包所需的 AWSConfig 策略

ConfigConformsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 7 月 25 日 21:38 UTC
- 编辑时间：2023 年 1 月 12 日 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CostOptimizationHubAdminAccess

描述：此托管策略为管理员提供对成本优化中心的访问权限。

CostOptimizationHubAdminAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CostOptimizationHubAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 19 日 00:03
- 编辑时间：世界标准时间 2023 年 12 月 19 日 00:03
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CostOptimizationHubReadOnlyAccess

描述：此托管策略提供对成本优化中心的只读访问权限。

CostOptimizationHubReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 CostOptimizationHubReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 13 日 18:04
- 编辑时间：世界标准时间 2023 年 12 月 13 日 18:04

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CostOptimizationHubServiceRolePolicy

描述：允许成本优化中心检索组织信息并收集与优化相关的数据和元数据。

CostOptimizationHubServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 08:03
- 编辑时间：世界标准时间 2023 年 11 月 26 日 08:03
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```



```
{
  "Sid" : "CostExplorerAccess",
  "Effect" : "Allow",
  "Action" : [
    "ce:ListCostAllocationTags"
  ],
  "Resource" : [
    "*"
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CustomerProfilesServiceLinkedRolePolicy

描述：允许 Amazon Connect 客户档案代表您访问 AWS 服务和资源。

CustomerProfilesServiceLinkedRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 7 日 22:56 UTC
- 编辑时间：2023 年 3 月 7 日 22:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DatabaseAdministrator

描述：授予对设置和配置 AWS 数据库 AWS 服务所需的服务和操作的完全访问权限。

DatabaseAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 DatabaseAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:25 UTC
- 编辑时间：2019 年 1 月 8 日 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ]
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DataScientist

描述：向 AWS 数据分析服务授予权限。

DataScientist 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 DataScientist 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:28 UTC
- 编辑时间：2019 年 12 月 3 日 16:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DAXServiceRolePolicy

描述：此策略允许 DAX 代表客户创建和管理网络接口、安全组、子网和 Vpc

DAXServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 5 日 17:51 UTC
- 编辑时间：2018 年 3 月 5 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

描述：支持亚马逊 DynamoDB 的亚马逊 CloudWatch 贡献者见解所需的权限。

DynamoDBCloudWatchContributorInsightsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 15 日 21:13 UTC
- 编辑时间：2019 年 11 月 15 日 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
    }  
  ]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DynamoDBKinesisReplicationServiceRolePolicy

描述：提供 AWS DynamoDB 访问权限 KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 12 日 00:43 UTC
- 编辑时间：2020 年 11 月 12 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

DynamoDBReplicationServiceRolePolicy

描述：DynamoDB 跨区域数据复制所需的权限

DynamoDBReplicationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2017 年 11 月 9 日 23:55 UTC
- 编辑时间：世界标准时间 2024 年 1 月 8 日 20:10
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2FastLaunchFullAccess

描述：此策略授予对 EC2 快速启动操作的完全访问权限

EC2FastLaunchFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 EC2FastLaunchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 5 月 13 日 22:45
- 编辑时间：世界标准时间 2024 年 5 月 13 日 22:45

- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "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/*"
  ]
},
{
  "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/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
```

```
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  },
  {
    "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2FastLaunchServiceRolePolicy

描述：政策允许 ec2fastlaunch 在客户账户中准备和管理预先配置的快照并发布相关指标。

EC2FastLaunchServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 1 月 10 日 13:08 UTC
- 编辑时间：2022 年 1 月 10 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  },
  {
    "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"
        ]
      }
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateLaunchTemplate",
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  },
  {
    "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"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots",
```

```
    "ec2:DescribeSubnets",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/EC2"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2FleetTimeShiftableServiceRolePolicy

描述：授予 EC2 队列在将来启动实例的权限的策略。

EC2FleetTimeShiftableServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2019 年 12 月 23 日 19:47 UTC
- 编辑时间 : 2019 年 12 月 23 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
        }
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Ec2ImageBuilderCrossAccountDistributionAccess

描述：EC2 Image Builder 执行跨账户分配所需的权限。

Ec2ImageBuilderCrossAccountDistributionAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `Ec2ImageBuilderCrossAccountDistributionAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 19:22 UTC
- 编辑时间：2020 年 9 月 30 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2ImageBuilderLifecycleExecutionPolicy

描述：EC2 ImageBuilderLifecycleExecutionPolicy 策略授予 Image Builder 执行诸如弃用或删除 Image Builder 图像资源及其底层资源（AMI、快照）等操作的权限，以支持图像生命周期管理任务的自动规则。

EC2ImageBuilderLifecycleExecutionPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 EC2ImageBuilderLifecycleExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2023 年 11 月 16 日 23:23
- 编辑时间：世界标准时间 2023 年 11 月 16 日 23:23
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2InstanceConnect

描述：允许客户调用 EC2 Instance Connect 向其 EC2 实例发布临时密钥，并通过 ssh 或 EC2 Instance Connect CLI 进行连接。

EC2InstanceConnect 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 EC2InstanceConnect 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 18:53 UTC
- 编辑时间：2019 年 6 月 27 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceConnect

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ]
    }
  ]
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Ec2InstanceConnectEndpoint

描述：用于管理客户创建的 EC2 Instance Connect 终端节点的 EC2 Instance Connect 终端节点策略

Ec2InstanceConnectEndpoint 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 1 月 24 日 20:19 UTC
- 编辑时间：2023 年 1 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2InstanceProfileForImageBuilder

描述：Image Builder 服务的 EC2 实例配置文件。

EC2InstanceProfileForImageBuilder 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 EC2InstanceProfileForImageBuilder 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 1 日 19:08 UTC
- 编辑时间：2020 年 8 月 27 日 16:40 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "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/*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

描述：用于使用 EC2 Image Builder 构建容器映像的 EC2 实例配置文件。此策略向用户授予上传 ECR 映像的广泛权限。

EC2InstanceProfileForImageBuilderECRContainerBuilds 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 EC2InstanceProfileForImageBuilderECRContainerBuilds 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 11 日 19:48 UTC
- 编辑时间：2020 年 12 月 11 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ECRReplicationServiceRolePolicy

描述：允许访问 ECR Replication AWS 服务 以及使用或管理的资源

ECRReplicationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 4 日 22:11 UTC
- 编辑时间：2020 年 12 月 4 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr:ReplicateImage"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElastiCacheServiceRolePolicy

描述：此政策 ElastiCache 允许在必要时代表您管理 AWS 资源，以管理您的缓存

ElastiCacheServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 12 月 7 日 17:50 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 03:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AmazonElasticCacheManaged" : "true"
        }
    }
},
{
    "Sid" : "ModifyVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/AmazonElasticCacheManaged" : "true"
        }
    }
},
{
    "Sid" : "AllowAccessToElasticCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElasticLoadBalancingFullAccess

描述：提供对 Amazon 的完全访问权限 ElasticLoadBalancing，以及对提供 ElasticLoadBalancing 功能所需的其他服务的有限访问权限。

ElasticLoadBalancingFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElasticLoadBalancingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 9 月 20 日 20:42 UTC
- 编辑时间：2022 年 11 月 29 日 01:45 UTC
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElasticLoadBalancingReadOnly

描述：提供对 Amazon ElasticLoadBalancing 和相关服务的只读访问权限

ElasticLoadBalancingReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 ElasticLoadBalancingReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 9 月 20 日 20:17 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 18:15
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalActivationsDownloadSoftwareAccess

说明：可以查看已购买的资产并下载相关软件和kickstart文件

ElementalActivationsDownloadSoftwareAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 ElementalActivationsDownloadSoftwareAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 8 日 17:26 UTC
- 编辑时间：2020 年 9 月 8 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "elemental-activations:Get*",
      "elemental-activations:Download*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalActivationsFullAccess

描述：查看元素设备和软件购买的资产并对其采取行动的完全访问权限

ElementalActivationsFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalActivationsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 4 日 21:00 UTC
- 编辑时间：2020 年 6 月 4 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalActivationsGenerateLicenses

描述：可以查看已购买的资产并生成待激活的软件许可证

ElementalActivationsGenerateLicenses 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalActivationsGenerateLicenses 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 28 日 18:28 UTC

- 编辑时间：2020 年 8 月 28 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalActivationsReadOnlyAccess

描述：对与用户关联的已购买资产的详细列表 AWS 账户 的只读访问权限

ElementalActivationsReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalActivationsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 28 日 16:51 UTC
- 编辑时间：2020 年 8 月 28 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalAppliancesSoftwareFullAccess

描述：查看元素设备和软件报价和订单并对其采取行动的完全访问权限

ElementalAppliancesSoftwareFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalAppliancesSoftwareFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 31 日 16:28 UTC
- 编辑时间：2021 年 2 月 5 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
```

```
        "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
  }
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalAppliancesSoftwareReadOnlyAccess

描述：只读访问权限，可查看 Elemental Appliances 和软件报价和订单

ElementalAppliancesSoftwareReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalAppliancesSoftwareReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 1 日 22:31 UTC
- 编辑时间：2020 年 4 月 1 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ElementalSupportCenterFullAccess

描述：查看 Elemental Appliance 和 Software 支持案例以及产品支持内容并采取行动的完全访问权限

ElementalSupportCenterFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ElementalSupportCenterFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 25 日 18:08 UTC
- 编辑时间：2021 年 2 月 5 日 21:02 UTC

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

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

EMRDescribeClusterPolicyForEMRWAL

描述：此策略授予只读权限，允许 Amazon EMR 的 WAL 服务查找并返回集群的状态

EMRDescribeClusterPolicyForEMRWAL 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 15 日 23:30 UTC
- 编辑时间：2023 年 6 月 15 日 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

FMSServiceRolePolicy

描述：允许调频服务关联角色对客户组织账户内的 FM 管理的资源执行与 FM 相关的操作的访问策略。
AWS

FMSServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 28 日 23:01 UTC
- 编辑时间：世界标准时间 2024 年 4 月 22 日 19:12
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

策略版本

策略版本：v29 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
}
```

```
    "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"
  ],
  "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",
```

```
    "iam: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:PutResourcePolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall>DeleteResourcePolicy",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:UpdateLoggingConfiguration"
  ],
  "Resource" : "*"
},
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

FSxDeleteServiceLinkedRoleAccess

描述：允许 Amazon FSx 删除其用于访问 Amazon S3 的服务关联角色

FSxDeleteServiceLinkedRoleAccess 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 28 日 10:40 UTC
- 编辑时间：2018 年 11 月 28 日 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GameLiftGameServerGroupPolicy

描述：允许 Gamelift 管理 GameServerGroups 客户资源的政策

GameLiftGameServerGroupPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GameLiftGameServerGroupPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 3 日 23:12 UTC
- 编辑时间：2020 年 5 月 13 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GlobalAcceleratorFullAccess

描述：允许 GlobalAccelerator 用户完全访问所有 API

GlobalAcceleratorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GlobalAcceleratorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 02:44 UTC
- 编辑时间：2020 年 12 月 4 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GlobalAcceleratorReadOnlyAccess

描述：允许 GlobalAccelerator 用户访问只读 API

GlobalAcceleratorReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GlobalAcceleratorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 02:41 UTC
- 编辑时间：2018 年 11 月 27 日 02:41 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GreengrassOTAUpdateArtifactAccess

描述：提供对所有 Greengrass 区域的 Greengrass OTA 更新工件的读取权限

GreengrassOTAUpdateArtifactAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GreengrassOTAUpdateArtifactAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 29 日 18:11 UTC
- 编辑时间：2018 年 12 月 18 日 00:59 UTC

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

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GroundTruthSyntheticConsoleFullAccess

描述 : 此政策授予使用 G SageMaker round Truth 合成控制台所有功能所需的权限。

GroundTruthSyntheticConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GroundTruthSyntheticConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 25 日 15:58 UTC
- 编辑时间：2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

GroundTruthSyntheticConsoleReadOnlyAccess

描述：此政策授予通过对 G SageMaker round Truth Synthetic 的只读访问权限 AWS Management Console。

GroundTruthSyntheticConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 GroundTruthSyntheticConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 25 日 15:58 UTC
- 编辑时间：2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Health_OrganizationsServiceRolePolicy

描述：启用“组织视图”功能的 Health_OrganizationsServiceRolePolicy 策略

Health_OrganizationsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 16 日 13:28 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 16:07
- ARN: arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMAccessAdvisorReadOnly

描述：此策略授予读取 IAM 访问顾问提供的所有访问信息的权限，例如上次访问的服务信息。

IAMAccessAdvisorReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMAccessAdvisorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 21 日 19:33 UTC
- 编辑时间：2019 年 6 月 21 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMAccessAnalyzerFullAccess

描述：提供对 IAM 访问分析器的完全访问权限

IAMAccessAnalyzerFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMAccessAnalyzerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 2 日 17:12 UTC
- 编辑时间：2019 年 12 月 2 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```



```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMAccessAnalyzerReadOnlyAccess

描述：提供对 IAM 访问分析器资源的只读访问权限

IAMAccessAnalyzerReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMAccessAnalyzerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 2 日 17:12 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 02:24
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "access-analyzer:CheckAccessNotGranted",
      "access-analyzer:CheckNoNewAccess",
      "access-analyzer:Get*",
      "access-analyzer:List*",
      "access-analyzer:ValidatePolicy"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMFullAccess

描述：通过提供对 IAM 的完全访问权限 AWS Management Console。

IAMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 6 月 21 日 19:40 UTC

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

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMReadOnlyAccess

描述：通过提供对 IAM 的只读访问权限 AWS Management Console。

IAMReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 1 月 25 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ]
    }
  ]
}
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMSelfManageServiceSpecificCredentials

描述：允许 IAM 用户管理自己的服务专用证书。

IAMSelfManageServiceSpecificCredentials 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMSelfManageServiceSpecificCredentials 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 22 日 17:25 UTC
- 编辑时间：2016 年 12 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMUserChangePassword

描述：让 IAM 用户能够更改自己的密码。

IAMUserChangePassword 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMUserChangePassword 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2016 年 11 月 15 日 00:25 UTC
- 编辑时间：2016 年 11 月 15 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

IAMUserSSHKeys

描述：让 IAM 用户能够管理自己的 SSH 密钥。

IAMUserSSHKeys 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IAMUserSSHKeys 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:08 UTC
- 编辑时间：2015 年 7 月 9 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IVSFullAccess

描述：提供对交互式视频服务 (IVS) 的完全访问权限，还包括完全访问 ivs 控制台所需的依赖服务的权限。

IVSFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IVSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 13 日 21:20
- 编辑时间：世界标准时间 2023 年 12 月 13 日 21:20
- ARN: arn:aws:iam::aws:policy/IVSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IVSReadOnlyAccess

描述：提供对 IVS 低延迟和实时直播 API 的只读访问权限

IVSReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 IVSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 5 日 18:00

- 编辑时间：世界标准时间 2024 年 2 月 16 日 18:03
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
```

```
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IVSRecordToS3

描述：服务关联角色，用于执行 S3 PutObject 以录制 IVS 直播

IVSRecordToS3是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 5 日 00:10 UTC
- 编辑时间：2020 年 12 月 5 日 00:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

KafkaConnectServiceRolePolicy

描述：此策略授予 Kafka Connect 代表您管理 AWS 资源的权限。

KafkaConnectServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 7 日 13:12 UTC

- 编辑时间：2021 年 9 月 7 日 13:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

KafkaServiceRolePolicy

描述：Kafka 的 IAM 服务关联角色策略。

KafkaServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 15 日 23:31 UTC
- 编辑时间：2023 年 4 月 28 日 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

KeyspacesReplicationServiceRolePolicy

描述：Keyspaces 跨区域数据复制所需的权限

KeyspacesReplicationServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 5 月 2 日 16:15 UTC
- 编辑时间：2023 年 5 月 2 日 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

LakeFormationDataAccessServiceRolePolicy

描述：授予对 Lake Formation 资源的临时数据访问权限的政策

LakeFormationDataAccessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 20 日 20:46 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 18:37
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Sid" : "LakeFormationDataAccessServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : [
    "arn:aws:s3:::*"
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

LexBotPolicy

描述：AWS Lex Bot 用例的策略

LexBotPolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 2 月 17 日 22:18 UTC
- 编辑时间：2019 年 11 月 13 日 22:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

LexChannelPolicy

描述：AWS Lex Channel 用例的政策

LexChannelPolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 2 月 17 日 23:23 UTC
- 编辑时间：2017 年 2 月 17 日 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

LightsailExportAccess

描述：AWS Lightsail 服务关联角色策略，用于授予资源导出权限

LightsailExportAccess 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 9 月 28 日 16:35 UTC
- 编辑时间：2022 年 1 月 15 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MediaConnectGatewayInstanceRolePolicy

描述：此策略授予向 MediaConnect 网关注册网关实例的 MediaConnect 权限。

MediaConnectGatewayInstanceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 MediaConnectGatewayInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 22 日 20:43 UTC
- 编辑时间：2023 年 3 月 22 日 20:43 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediacconnect:DiscoverGatewayPollEndpoint",
        "mediacconnect:PollGateway",
        "mediacconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MediaPackageServiceRolePolicy

描述 : 允许 MediaPackage 将日志发布到 CloudWatch

MediaPackageServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 9 月 18 日 17:45 UTC
- 编辑时间：2020 年 9 月 18 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MemoryDBServiceRolePolicy

描述：此策略允许 MemoryDB 在必要时代表您管理 AWS 资源，以管理您的资源。

MemoryDBServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 17 日 22:34 UTC
- 编辑时间：2021 年 8 月 18 日 23:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Action" : [
  "ec2:CreateTags"
],
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : "CreateNetworkInterface"
  },
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AmazonMemoryDBManaged"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ]
}
```

```
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/MemoryDB"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MigrationHubDMSAccessServiceRolePolicy

描述：数据库迁移服务的策略，即在客户账户中扮演角色以调用 Migration Hub

MigrationHubDMSAccessServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 12 日 17:50 UTC
- 编辑时间：2019 年 10 月 7 日 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MigrationHubServiceRolePolicy

描述：允许 Migration Hub 代表你调用 Application Discovery Service

MigrationHubServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 12 日 17:22 UTC
- 编辑时间：2020 年 8 月 6 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MigrationHubSMSAccessServiceRolePolicy

描述：服务器迁移服务在客户账户中扮演角色以调用 Migration Hub 的政策

MigrationHubSMSAccessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 12 日 18:30 UTC
- 编辑时间：2019 年 10 月 7 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

MonitronServiceRolePolicy

描述：授予对所需客户 AWS 资源的访问权限的 Monitron 服务关联角色的策略。

MonitronServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 5 月 2 日 19:22 UTC
- 编辑时间：2022 年 5 月 2 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/monitron/*"
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

NeptuneConsoleFullAccess

描述：提供使用管理 Amazon Neptune 的完全访问权限。AWS Management Console 请注意，此策略还授予向账户内的所有 SNS 主题发布的完全访问权限，创建和编辑 Amazon EC2 实例及 VPC 配置的权限，在 Amazon KMS 上查看和列出密钥的权限以及对 Amazon RDS 的完全访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

NeptuneConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 NeptuneConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 19 日 21:35 UTC
- 编辑时间：世界标准时间 2023 年 11 月 30 日 07:32
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AllowOtherDependentPermissions",
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

NeptuneFullAccess

描述：提供对亚马逊 Neptune 的完全访问权限。请注意，此策略还授予向账户内的所有 SNS 主题发布的完全访问权限和对 Amazon RDS 的完全访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

NeptuneFullAccess是一个[AWS 托管策略](#)。

使用此策略

您可以将 NeptuneFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 30 日 19:17 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 16:32
- ARN: arn:aws:iam::aws:policy/NeptuneFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AllowOtherDependentPermissions",
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

NeptuneGraphReadOnlyAccess

描述：提供对所有 Amazon Neptune Analytics 资源的只读访问权限以及依赖服务的只读权限。

NeptuneGraphReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 NeptuneGraphReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 30 日 07:32
- 编辑时间：世界标准时间 2023 年 11 月 30 日 07:32
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

NeptuneReadOnlyAccess

描述：提供对亚马逊 Neptune 的只读访问权限。请注意，此策略还授予对 Amazon RDS 资源的访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

NeptuneReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 NeptuneReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 30 日 19:16 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 16:33
- ARN: arn:aws:iam::aws:policy/NeptuneReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

NetworkAdministrator

描述：授予设置和配置 AWS 网络资源所需的 AWS 服务和操作的完全访问权限。

NetworkAdministrator 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 NetworkAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:31 UTC
- 编辑时间：2021 年 9 月 16 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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:DescribeKeyPairs",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"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:DescribePublicIpv4Pools",
```

```
"ec2:DescribeIpv6Pools",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:DisassociateSubnetCidrBlock",
"ec2:DisassociateVpcCidrBlock",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVpcClassicLinkDnsSupport",
"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:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceNetworkAclEntry",
"ec2:ReplaceRoute",
"ec2:ReplaceRouteTableAssociation",
"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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AcceptVpcPeeringConnection",
    "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:DetachClassicLinkVpc",
    "ec2:DisableVpcClassicLink",
    "ec2:EnableVpcClassicLink",
    "ec2:GetConsoleScreenshot",
    "ec2:RejectVpcPeeringConnection",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "s3:ListBucket"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/flow-logs-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "networkmanager:*"
  ],
  "Resource" : "*"
},
{
  "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:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "transitgateway.amazonaws.com"
      ]
    }
  }
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

OAMFullAccess

描述：提供对可 CloudWatch 观察性访问管理器的完全访问权限

OAMFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 OAMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:38 UTC
- 编辑时间：2022 年 11 月 27 日 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "oam:*"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

OAMReadOnlyAccess

描述：提供对可 CloudWatch 观察性访问管理器的只读访问权限

OAMReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 OAMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:29 UTC
- 编辑时间：2022 年 11 月 27 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

OpensearchIngestionSelfManagedVpcePolicy

描述：允许 Amazon OpenSearch Ingestion 描述网络资源并将服务指标写入 cloudwatch

OpensearchIngestionSelfManagedVpcePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：世界标准时间 2024 年 6 月 10 日 19:59
- 编辑时间：世界标准时间 2024 年 6 月 10 日 19:59
- ARN: arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

PartnerCentralAccountManagementUserRoleAssociation

描述：提供将合作伙伴中心用户与 IAM 角色关联和解除关联的权限

PartnerCentralAccountManagementUserRoleAssociation 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 PartnerCentralAccountManagementUserRoleAssociation 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 11 月 10 日 02:03 UTC
- 编辑时间：2023 年 11 月 10 日 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

PowerUserAccess

描述：提供对 AWS 服务和资源的完全访问权限，但不允许管理用户和群组。

PowerUserAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 PowerUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 7 月 6 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole",
        "iam>DeleteServiceLinkedRole",
        "iam>ListRoles",
        "organizations:DescribeOrganization",
        "account:ListRegions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

QBusinessServiceRolePolicy

描述：向 Amazon Q 授予权限 AWS 服务 和使用或管理的资源

QBusinessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 4 月 29 日 16:05
- 编辑时间：世界标准时间 2024 年 4 月 29 日 16:05
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

描述：QuickSight 团队用于访问 S3 存储管理分析生成的客户数据的策略。

QuickSightAccessForS3StorageManagementAnalyticsReadOnly 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 QuickSightAccessForS3StorageManagementAnalyticsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 6 月 12 日 18:18 UTC
- 编辑时间：2019 年 10 月 8 日 23:53 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

RDSCloudHsmAuthorizationRole

描述：Amazon RDS 服务角色的默认策略。

RDSCloudHsmAuthorizationRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 RDSCloudHsmAuthorizationRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2019 年 9 月 26 日 22:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",

```

```
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ReadOnlyAccess

描述：提供对 AWS 服务和资源的只读访问权限。

ReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：世界标准时间 2024 年 5 月 16 日 21:10
- ARN: arn:aws:iam::aws:policy/ReadOnlyAccess

策略版本

策略版本：v113 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "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: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:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "airflow:ListEnvironments",
      ]
    }
  ]
}
```

```
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:GetDomainAssociation",
"amplify:GetJob",
"amplify:ListApps",
"amplify:ListBranches",
"amplify:ListDomainAssociations",
"amplify:ListJobs",
"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:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"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",
"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*",
"appsync:Get*",
```

```
"appsync:List*",
"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:GetManagedResource",
"arc-zonal-shift:ListAutoshifts",
"arc-zonal-shift:ListManagedResources",
"arc-zonal-shift:ListZonalShifts",
"artifact:GetReport",
"artifact:GetReportMetadata",
"artifact:GetTermForReport",
"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:GetAgentKnowledgeBase",
"bedrock:GetAgentVersion",
"bedrock:GetCustomModel",
"bedrock:GetDataSource",
"bedrock:GetFoundationModel",
"bedrock:GetFoundationModelAvailability",
"bedrock:GetIngestionJob",
"bedrock:GetKnowledgeBase",
"bedrock:GetModelCustomizationJob",
```

```
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:GetProvisionedModelThroughput",
"bedrock:GetUseCaseForModelAccess",
"bedrock:ListAgentActionGroups",
"bedrock:ListAgentAliases",
"bedrock:ListAgentKnowledgeBases",
"bedrock:ListAgents",
"bedrock:ListAgentVersions",
"bedrock:ListCustomModels",
"bedrock:ListDataSources",
"bedrock:ListFoundationModelAgreementOffers",
"bedrock:ListFoundationModels",
"bedrock:ListIngestionJobs",
"bedrock:ListKnowledgeBases",
"bedrock:ListModelCustomizationJobs",
"bedrock:ListProvisionedModelThroughputs",
"billing:GetBillingData",
"billing:GetBillingDetails",
"billing:GetBillingNotifications",
"billing:GetBillingPreferences",
"billing:GetContractInformation",
"billing:GetCredits",
"billing:GetIAMAccessPreference",
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"billingconductor:GetBillingGroupCostReport",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroupCostReports",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListCustomLineItemVersions",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingPlansAssociatedWithPricingRule",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListResourcesAssociatedToCustomLineItem",
"billingconductor:ListTagsForResource",
"braket:GetDevice",
"braket:GetJob",
"braket:GetQuantumTask",
"braket:SearchDevices",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"budgets:Describe*",
```

```
"budgets:View*",
"cassandra:Select",
"ce:DescribeCostCategoryDefinition",
"ce:DescribeNotificationSubscription",
"ce:DescribeReport",
"ce:GetAnomalies",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"ce:GetApproximateUsageRecords",
"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:ListCostAllocationTags",
"ce:ListCostAllocationTagBackfillHistory",
"ce:ListCostCategoryDefinitions",
"ce:ListSavingsPlansPurchaseRecommendationGeneration",
"ce:ListTagsForResource",
"chatbot:Describe*",
"chatbot:Get*",
"chatbot:ListMicrosoftTeamsChannelConfigurations",
"chatbot:ListMicrosoftTeamsConfiguredTeams",
"chatbot:ListMicrosoftTeamsUserIdentities",
"chime:Get*",
"chime:List*",
"chime:Retrieve*",
"chime:Search*",
"chime:Validate*",
"cleanrooms:BatchGetCollaborationAnalysisTemplate",
"cleanrooms:BatchGetSchema",
"cleanrooms:GetAnalysisTemplate",
```

```
"cleanrooms:GetCollaboration",
"cleanrooms:GetCollaborationAnalysisTemplate",
"cleanrooms:GetConfiguredAudienceModelAssociation",
"cleanrooms:GetConfiguredTable",
"cleanrooms:GetConfiguredTableAnalysisRule",
"cleanrooms:GetConfiguredTableAssociation",
"cleanrooms:GetMembership",
"cleanrooms:GetProtectedQuery",
"cleanrooms:GetSchema",
"cleanrooms:GetSchemaAnalysisRule",
"cleanrooms:ListAnalysisTemplates",
"cleanrooms:ListCollaborationAnalysisTemplates",
"cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
"cleanrooms:ListCollaborations",
"cleanrooms:ListConfiguredTableAssociations",
"cleanrooms:ListConfiguredTables",
"cleanrooms:ListMembers",
"cleanrooms:ListMemberships",
"cleanrooms:ListProtectedQueries",
"cleanrooms:ListSchemas",
"cleanrooms:ListTagsForResource",
"cleanrooms-ml:GetTrainingDataset",
"cleanrooms-ml:GetAudienceGenerationJob",
"cleanrooms-ml:GetAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModelPolicy",
"cleanrooms-ml:ListAudienceExportJobs",
"cleanrooms-ml:ListAudienceGenerationJobs",
"cleanrooms-ml:ListAudienceModels",
"cleanrooms-ml:ListConfiguredAudienceModels",
"cleanrooms-ml:ListTrainingDatasets",
"cleanrooms-ml:ListTagsForResource",
"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:ListPackages",
"codeartifact:ListPackageVersionAssets",
"codeartifact:ListPackageVersionDependencies",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListRepositoriesInDomain",
"codeartifact:ListTagsForResource",
"codeartifact:ReadFromRepository",
"codebuild:BatchGet*",
"codebuild:DescribeCodeCoverages",
"codebuild:DescribeTestCases",
"codebuild:List*",
"codecatalyst:GetBillingAuthorization",
"codecatalyst:GetConnection",
"codecatalyst:GetPendingConnection",
```

```
"codecatalyst:ListConnections",
"codecatalyst:ListIamRolesForConnection",
"codecatalyst:ListTagsForResource",
"codecommit:BatchGet*",
"codecommit:Describe*",
"codecommit:Get*",
"codecommit:GitPull",
"codecommit:List*",
"codedeploy:BatchGet*",
"codedeploy:Get*",
"codedeploy:List*",
"codeguru-profiler:Describe*",
"codeguru-profiler:Get*",
"codeguru-profiler:List*",
"codeguru-reviewer:Describe*",
"codeguru-reviewer:Get*",
"codeguru-reviewer:List*",
"codepipeline:Get*",
"codepipeline:List*",
"codestar-connections:GetConnection",
"codestar-connections:GetHost",
"codestar-connections:GetRepositoryLink",
"codestar-connections:GetRepositorySyncStatus",
"codestar-connections:GetResourceSyncStatus",
"codestar-connections:GetSyncConfiguration",
"codestar-connections:ListConnections",
"codestar-connections:ListHosts",
"codestar-connections:ListRepositoryLinks",
"codestar-connections:ListRepositorySyncDefinitions",
"codestar-connections:ListSyncConfigurations",
"codestar-connections:ListTagsForResource",
"codestar-notifications:describeNotificationRule",
"codestar-notifications:listEventTypes",
"codestar-notifications:listNotificationRules",
"codestar-notifications:listTagsForResource",
"codestar-notifications:ListTargets",
"codestar:Describe*",
"codestar:Get*",
"codestar:List*",
"codestar:Verify*",
"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:GetLambdaFunctionRecommendations",
"compute-optimizer:GetLicenseRecommendations",
"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",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendations",
"cost-optimization-hub:ListRecommendationSummaries",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"customer-verification:GetCustomerVerificationDetails",
"customer-verification:GetCustomerVerificationEligibility",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeJobRun",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobRuns",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"databrew:ListTagsForResource",
"dataexchange:Get*",
"dataexchange:List*",
"datapipeline:Describe*",
"datapipeline:EvaluateExpression",
"datapipeline:Get*",
```

```
"datapipeline:List*",
"datapipeline:QueryObjects",
"datapipeline:Validate*",
"datasync:Describe*",
"datasync:List*",
"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: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*",
"dynamodb:BatchGet*",
"dynamodb:Describe*",
"dynamodb:Get*",
"dynamodb:List*",
"dynamodb: PartiQLSelect",
"dynamodb:Query",
"dynamodb:Scan",
```

```
"ec2:Describe*",
"ec2:Get*",
"ec2:ListImagesInRecycleBin",
"ec2:ListSnapshotsInRecycleBin",
"ec2:SearchLocalGatewayRoutes",
"ec2:SearchTransitGatewayRoutes",
"ec2messages:Get*",
"ecr-public:BatchCheckLayerAvailability",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetAuthorizationToken",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchCheck*",
"ecr:BatchGet*",
"ecr:Describe*",
"ecr:Get*",
"ecr:List*",
"ecs:Describe*",
"ecs:List*",
"eks:Describe*",
"eks:List*",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:ListTagsForResource",
"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:ListExperiments",
"fis:ListExperimentTargetAccountConfigurations",
"fis:ListExperimentTemplates",
"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:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypeTypes",
"frauddetector:GetEvent",
"frauddetector:GetEventPredictionMetadata",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetKMSEncryptionKey",
"frauddetector:GetLabels",
"frauddetector:GetListElements",
"frauddetector:GetListsMetadata",
"frauddetector:GetModels",
"frauddetector:GetModelVersion",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListEventPredictions",
"frauddetector:ListTagsForResource",
"freertos:Describe*",
"freertos:List*",
"freetier: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:BatchGetTriggers",
"glue:BatchGetWorkflows",
"glue:CheckSchemaVersionValidity",
"glue:GetCatalogImportStatus",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlerMetrics",
"glue:GetCrawlers",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDataflowGraph",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobBookmark",
"glue:GetJobRun",
"glue:GetJobRuns",
"glue:GetJobs",
"glue:GetMapping",
"glue:GetMLTaskRun",
"glue:GetMLTaskRuns",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetPlan",
"glue:GetRegistry",
"glue:GetResourcePolicy",
"glue:GetSchema",
```

```
"glue:GetSchemaByDefinition",
"glue:GetSchemaVersion",
"glue:GetSchemaVersionsDiff",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersion",
"glue:GetTableVersions",
"glue:GetTags",
"glue:GetTrigger",
"glue:GetTriggers",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions",
"glue:GetWorkflow",
"glue:GetWorkflowRun",
"glue:GetWorkflowRunProperties",
"glue:GetWorkflowRuns",
"glue:ListCrawlers",
"glue:ListCrawls",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
"glue:ListRegistries",
"glue:ListSchemas",
"glue:ListSchemaVersions",
"glue: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*",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"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",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetInternetEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"internetmonitor:ListInternetEvents",
"internetmonitor:ListMonitors",
"internetmonitor:ListTagsForResource",
"invoicing:GetInvoiceEmailDeliveryPreferences",
"invoicing:GetInvoicePDF",
"invoicing:ListInvoiceSummaries",
"iot:Describe*",
"iot:Get*",
"iot:List*",
"iot1click:DescribeDevice",
"iot1click:DescribePlacement",
"iot1click:DescribeProject",
"iot1click:GetDeviceMethods",
"iot1click:GetDevicesInPlacement",
"iot1click:ListDeviceEvents",
```

```
"iot1click:ListDevices",
"iot1click:ListPlacements",
"iot1click:ListProjects",
"iot1click:ListTagsForResource",
"iotanalytics:Describe*",
"iotanalytics:Get*",
"iotanalytics:List*",
"iotanalytics:SampleChannelData",
"iotevents:DescribeAlarm",
"iotevents:DescribeAlarmModel",
"iotevents:DescribeDetector",
"iotevents:DescribeDetectorModel",
"iotevents:DescribeInput",
"iotevents:DescribeLoggingOptions",
"iotevents:ListAlarmModels",
"iotevents:ListAlarmModelVersions",
"iotevents:ListAlarms",
"iotevents:ListDetectorModels",
"iotevents:ListDetectorModelVersions",
"iotevents:ListDetectors",
"iotevents:ListInputs",
"iotevents:ListTagsForResource",
"iotfleethub:DescribeApplication",
"iotfleethub:ListApplications",
"iotfleetwise:GetCampaign",
"iotfleetwise:GetDecoderManifest",
"iotfleetwise:GetFleet",
"iotfleetwise:GetLoggingOptions",
"iotfleetwise:GetModelManifest",
"iotfleetwise:GetRegisterAccountStatus",
"iotfleetwise:GetSignalCatalog",
"iotfleetwise:GetVehicle",
"iotfleetwise:GetVehicleStatus",
"iotfleetwise:ListCampaigns",
"iotfleetwise:ListDecoderManifestNetworkInterfaces",
"iotfleetwise:ListDecoderManifests",
"iotfleetwise:ListDecoderManifestSignals",
"iotfleetwise:ListFleets",
"iotfleetwise:ListFleetsForVehicle",
"iotfleetwise:ListModelManifestNodes",
"iotfleetwise:ListModelManifests",
"iotfleetwise:ListSignalCatalogNodes",
"iotfleetwise:ListSignalCatalogs",
"iotfleetwise:ListTagsForResource",
```



```
"iotfleetwise:ListVehicles",
"iotfleetwise:ListVehiclesInFleet",
"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:GetMetrics",
"iotwireless:GetMetricConfiguration",
"iotwireless:GetMulticastGroup",
"iotwireless:GetMulticastGroupSession",
"iotwireless:GetNetworkAnalyzerConfiguration",
"iotwireless:GetPartnerAccount",
"iotwireless:GetPosition",
"iotwireless:GetPositionConfiguration",
"iotwireless:GetPositionEstimate",
"iotwireless:GetResourceEventConfiguration",
"iotwireless:GetResourceLogLevel",
"iotwireless:GetResourcePosition",
"iotwireless:GetServiceEndpoint",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessDeviceImportTask",
"iotwireless:GetWirelessDeviceStatistics",
"iotwireless:GetWirelessGateway",
"iotwireless:GetWirelessGatewayCertificate",
"iotwireless:GetWirelessGatewayFirmwareInformation",
"iotwireless:GetWirelessGatewayStatistics",
"iotwireless:GetWirelessGatewayTask",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListDestinations",
"iotwireless:ListDeviceProfiles",
"iotwireless:ListDevicesForWirelessDeviceImportTask",
```

```
"iotwireless:ListEventConfigurations",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListMulticastGroupsByFuotaTask",
"iotwireless:ListNetworkAnalyzerConfigurations",
"iotwireless:ListPartnerAccounts",
"iotwireless:ListPositionConfigurations",
"iotwireless:ListQueuedMessages",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDeviceImportTasks",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGateways",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:BatchGetChannel",
"ivs:GetChannel",
"ivs:GetComposition",
"ivs:GetEncoderConfiguration",
"ivs:GetStage",
"ivs:GetStageSession",
"ivs:GetParticipant",
"ivs:GetPlaybackKeyPair",
"ivs:GetPlaybackRestrictionPolicy",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListCompositions",
"ivs:ListEncoderConfigurations",
"ivs:ListParticipants",
"ivs:ListParticipantEvents",
"ivs:ListPlaybackKeyPairs",
"ivs:ListPlaybackRestrictionPolicies",
"ivs:ListRecordingConfigurations",
"ivs:ListStages",
"ivs:ListStageSessions",
"ivs:ListStreams",
"ivs:ListStreamKeys",
"ivs:ListStreamSessions",
"ivs:ListTagsForResource",
"ivschat:GetLoggingConfiguration",
"ivschat:GetRoom",
"ivschat:ListLoggingConfigurations",
"ivschat:ListRooms",
"ivschat:ListTagsForResource",
```

```
"kafka:Describe*",
"kafka:DescribeCluster",
"kafka:DescribeClusterOperation",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:Get*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafka:ListClusterOperations",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurationRevisions",
"kafka:ListConfigurations",
"kafka:ListKafkaVersions",
"kafka:ListNodes",
"kafka:ListTagsForResource",
"kafkaconnect:DescribeConnector",
"kafkaconnect:DescribeCustomPlugin",
"kafkaconnect:DescribeWorkerConfiguration",
"kafkaconnect:ListConnectors",
"kafkaconnect:ListCustomPlugins",
"kafkaconnect:ListWorkerConfigurations",
"kendra:BatchGetDocumentStatus",
"kendra:DescribeDataSource",
"kendra:DescribeExperience",
"kendra:DescribeFaq",
"kendra:DescribeIndex",
"kendra:DescribePrincipalMapping",
"kendra:DescribeQuerySuggestionsBlockList",
"kendra:DescribeQuerySuggestionsConfig",
"kendra:DescribeThesaurus",
"kendra:GetQuerySuggestions",
"kendra:GetSnapshots",
"kendra:ListDataSources",
"kendra:ListDataSourceSyncJobs",
"kendra:ListEntityPersonas",
"kendra:ListExperienceEntities",
"kendra:ListExperiences",
"kendra:ListFaqs",
"kendra:ListGroupsOlderThanOrderingId",
"kendra:ListIndices",
"kendra:ListQuerySuggestionsBlockLists",
```

```
"kendra:ListTagsForResource",
"kendra:ListThesauri",
"kendra:Query",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kinesisanalytics:Describe*",
"kinesisanalytics:Discover*",
"kinesisanalytics:Get*",
"kinesisanalytics:List*",
"kinesisvideo:Describe*",
"kinesisvideo:Get*",
"kinesisvideo:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lakeformation:DescribeResource",
"lakeformation:GetDataCellsFilter",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetEffectivePermissionsForPath",
"lakeformation:GetLfTag",
"lakeformation:GetResourceLfTags",
"lakeformation:ListDataCellsFilter",
"lakeformation:ListLfTags",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lakeformation:ListTableStorageOptimizers",
"lakeformation:SearchDatabasesByLfTags",
"lakeformation:SearchTablesByLfTags",
"lambda:Get*",
"lambda:List*",
"launchwizard:DescribeAdditionalNode",
"launchwizard:DescribeProvisionedApp",
"launchwizard:DescribeProvisioningEvents",
"launchwizard:DescribeSettingsSet",
"launchwizard:GetDeployment",
"launchwizard:GetInfrastructureSuggestion",
"launchwizard:GetIpAddress",
"launchwizard:GetResourceCostEstimate",
"launchwizard:GetResourceRecommendation",
"launchwizard:GetSettingsSet",
"launchwizard:GetWorkload",
"launchwizard:GetWorkloadAsset",
"launchwizard:GetWorkloadAssets",
```

```
"launchwizard:ListAdditionalNodes",
"launchwizard:ListAllowedResources",
"launchwizard:ListDeploymentEvents",
"launchwizard:ListDeployments",
"launchwizard:ListProvisionedApps",
"launchwizard:ListResourceCostEstimates",
"launchwizard:ListSettingsSets",
"launchwizard:ListWorkloadDeploymentOptions",
"launchwizard:ListWorkloadDeploymentPatterns",
"launchwizard:ListWorkloads",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotChannel",
"lex:DescribeBotLocale",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:Get*",
"lex:ListBotAliases",
"lex:ListBotChannels",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
"lex:ListBuiltInIntents",
"lex:ListBuiltInSlotTypes",
"lex:ListExports",
"lex:ListImports",
"lex:ListIntents",
"lex:ListSlots",
"lex:ListSlotTypes",
"lex:ListTagsForResource",
"license-manager:Get*",
"license-manager:List*",
"lightsail:GetActiveNames",
"lightsail:GetAlarms",
"lightsail:GetAutoSnapshots",
"lightsail:GetBlueprints",
"lightsail:GetBucketAccessKeys",
"lightsail:GetBucketBundles",
"lightsail:GetBucketMetricData",
```

```
"lightsail:GetBuckets",
"lightsail:GetBundles",
"lightsail:GetCertificates",
"lightsail:GetCloudFormationStackRecords",
"lightsail:GetContainerAPIMetadata",
"lightsail:GetContainerImages",
"lightsail:GetContainerServiceDeployments",
"lightsail:GetContainerServiceMetricData",
"lightsail:GetContainerServicePowers",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshot",
"lightsail:GetDiskSnapshots",
"lightsail:GetDistributionBundles",
"lightsail:GetDistributionLatestCacheReset",
"lightsail:GetDistributionMetricData",
"lightsail:GetDistributions",
"lightsail:GetDomain",
"lightsail:GetDomains",
"lightsail:GetExportSnapshotRecords",
"lightsail:GetInstance",
"lightsail:GetInstanceMetricData",
"lightsail:GetInstancePortStates",
"lightsail:GetInstances",
"lightsail:GetInstanceSnapshot",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstanceState",
"lightsail:GetKeyPair",
"lightsail:GetKeyPairs",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancerMetricData",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetOperation",
"lightsail:GetOperations",
"lightsail:GetOperationsForResource",
"lightsail:GetRegions",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseBlueprints",
"lightsail:GetRelationalDatabaseBundles",
"lightsail:GetRelationalDatabaseEvents",
"lightsail:GetRelationalDatabaseLogEvents",
"lightsail:GetRelationalDatabaseLogStreams",
```

```
"lightsail:GetRelationalDatabaseMetricData",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetRelationalDatabaseSnapshot",
"lightsail:GetRelationalDatabaseSnapshots",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"lightsail:Is*",
"logs:Describe*",
"logs:FilterLogEvents",
"logs:Get*",
"logs:ListAnomalies",
"logs:ListLogAnomalyDetectors",
"logs:ListLogDeliveries",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"logs:StartLiveTail",
"logs:StartQuery",
"logs:StopLiveTail",
"logs:StopQuery",
"logs:TestMetricFilter",
"lookoutequipment:DescribeDataIngestionJob",
"lookoutequipment:DescribeDataset",
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:DescribeLabel",
"lookoutequipment:DescribeLabelGroup",
"lookoutequipment:DescribeModel",
"lookoutequipment:DescribeModelVersion",
"lookoutequipment:DescribeResourcePolicy",
"lookoutequipment:DescribeRetrainingScheduler",
"lookoutequipment:ListDataIngestionJobs",
"lookoutequipment:ListDatasets",
"lookoutequipment:ListInferenceEvents",
"lookoutequipment:ListInferenceExecutions",
"lookoutequipment:ListInferenceSchedulers",
"lookoutequipment:ListLabelGroups",
"lookoutequipment:ListLabels",
"lookoutequipment:ListModels",
"lookoutequipment:ListModelVersions",
"lookoutequipment:ListRetrainingSchedulers",
"lookoutequipment:ListSensorStatistics",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:Describe*",
"lookoutmetrics:Get*",
```

```
"lookoutmetrics:List*",
"lookoutvision:DescribeDataset",
"lookoutvision:DescribeModel",
"lookoutvision:DescribeModelPackagingJob",
"lookoutvision:DescribeProject",
"lookoutvision:ListDatasetEntries",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"lookoutvision:ListTagsForResource",
"m2:GetApplication",
"m2:GetApplicationVersion",
"m2:GetBatchJobExecution",
"m2:GetDataSetDetails",
"m2:GetDataSetImportTask",
"m2:GetDeployment",
"m2:GetEnvironment",
"m2:ListApplications",
"m2:ListApplicationVersions",
"m2:ListBatchJobDefinitions",
"m2:ListBatchJobExecutions",
"m2:ListDataSetImportHistory",
"m2:ListDataSets",
"m2:ListDeployments",
"m2:ListEngineVersions",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"machinelearning:Describe*",
"machinelearning:Get*",
"macie2:BatchGetCustomDataIdentifiers",
"macie2:DescribeBuckets",
"macie2:DescribeClassificationJob",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAdministratorAccount",
"macie2:GetAllowList",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetBucketStatistics",
"macie2:GetClassificationExportConfiguration",
"macie2:GetClassificationScope",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindings",
"macie2:GetFindingsFilter",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetFindingStatistics",
```



```
"macie2:GetInvitationsCount",
"macie2:GetMacieSession",
"macie2:GetMember",
"macie2:GetResourceProfile",
"macie2:GetRevealConfiguration",
"macie2:GetSensitiveDataOccurrencesAvailability",
"macie2:GetSensitivityInspectionTemplate",
"macie2:GetUsageStatistics",
"macie2:GetUsageTotals",
"macie2:ListAllowLists",
"macie2:ListClassificationJobs",
"macie2:ListClassificationScopes",
"macie2:ListCustomDataIdentifiers",
"macie2:ListFindings",
"macie2:ListFindingsFilters",
"macie2:ListInvitations",
"macie2:ListMembers",
"macie2:ListOrganizationAdminAccounts",
"macie2:ListResourceProfileArtifacts",
"macie2:ListResourceProfileDetections",
"macie2:ListSensitivityInspectionTemplates",
"macie2:ListTagsForResource",
"macie2:SearchResources",
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:GetProposal",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNetworks",
"managedblockchain:ListNodes",
"managedblockchain:ListProposals",
"managedblockchain:ListProposalVotes",
"managedblockchain:ListTagsForResource",
"mediaconnect:DescribeFlow",
"mediaconnect: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:ListInputDevices",
"medialive:ListInputDeviceTransfers",
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"medialive:ListSignalMaps",
"medialive:ListTagsForResource",
"mediapackage-vod:Describe*",
"mediapackage-vod:List*",
"mediapackage:Describe*",
"mediapackage:List*",
"mediapackagev2:GetChannel",
"mediapackagev2:GetChannelGroup",
"mediapackagev2:GetChannelPolicy",
"mediapackagev2:GetHeadObject",
"mediapackagev2:GetObject",
"mediapackagev2:GetOriginEndpoint",
"mediapackagev2:GetOriginEndpointPolicy",
"mediapackagev2:ListChannelGroups",
"mediapackagev2:ListChannels",
```

```
"mediapackagev2:ListOriginEndpoints",
"mediapackagev2:ListTagsForResource",
"mediastore:DescribeContainer",
"mediastore:DescribeObject",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:GetLifecyclePolicy",
"mediastore:GetMetricPolicy",
"mediastore:GetObject",
"mediastore:ListContainers",
"mediastore:ListItems",
"mediastore:ListTagsForResource",
"memorydb: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:ListTagsForResource",
"network-firewall:ListTLSInspectionConfigurations",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectAttachment",
"networkmanager:GetConnections",
"networkmanager:GetConnectPeer",
"networkmanager:GetConnectPeerAssociations",
"networkmanager:GetCoreNetwork",
"networkmanager:GetCoreNetworkChangeEvents",
"networkmanager:GetCoreNetworkChangeSet",
"networkmanager:GetCoreNetworkPolicy",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetNetworkResourceCounts",
"networkmanager:GetNetworkResourceRelationships",
"networkmanager:GetNetworkResources",
"networkmanager:GetNetworkRoutes",
"networkmanager:GetNetworkTelemetry",
"networkmanager:GetResourcePolicy",
"networkmanager:GetRouteAnalysis",
"networkmanager:GetSites",
"networkmanager:GetSiteToSiteVpnAttachment",
"networkmanager:GetTransitGatewayConnectPeerAssociations",
"networkmanager:GetTransitGatewayPeering",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:GetTransitGatewayRouteTableAttachment",
"networkmanager:GetVpcAttachment",
"networkmanager: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:GetNotificationConfiguration",
"notifications:GetNotificationEvent",
"notifications:ListChannels",
"notifications:ListEventRules",
"notifications:ListNotificationConfigurations",
"notifications:ListNotificationEvents",
"notifications:ListNotificationHubs",
"notifications:ListTagsForResource",
"oam:GetLink",
"oam:GetSink",
"oam:GetSinkPolicy",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"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:ListPaymentPreferences",
"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",
"personalize:Describe*",
"personalize:Get*",
"personalize:List*",
"pi:DescribeDimensionKeys",
"pi:GetDimensionKeyDetails",
"pi:GetResourceMetadata",
"pi:GetResourceMetrics",
```

```
"pi:ListAvailableResourceDimensions",
"pi:ListAvailableResourceMetrics",
"pipes:DescribePipe",
"pipes:ListPipes",
"pipes:ListTagsForResource",
"polly:Describe*",
"polly:Get*",
"polly:List*",
"polly:SynthesizeSpeech",
"pricing:DescribeServices",
"pricing:GetAttributeValues",
"pricing:GetPriceListFileUrl",
"pricing:GetProducts",
"pricing:ListPriceLists",
"proton:GetDeployment",
"proton:GetEnvironment",
"proton:GetEnvironmentTemplate",
"proton:GetEnvironmentTemplateVersion",
"proton:GetService",
"proton:GetServiceInstance",
"proton:GetServiceTemplate",
"proton:GetServiceTemplateVersion",
"proton:ListDeployments",
"proton:ListEnvironmentAccountConnections",
"proton:ListEnvironments",
"proton:ListEnvironmentTemplates",
"proton:ListServiceInstances",
"proton:ListServices",
"proton:ListServiceTemplates",
"proton:ListTagsForResource",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:ListPurchaseOrderInvoices",
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ViewPurchaseOrders",
"qldb:DescribeJournalKinesisStream",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:GetBlock",
"qldb:GetDigest",
"qldb:GetRevision",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
```

```
"qlldb:ListTagsForResource",
"ram:Get*",
"ram:List*",
"rbin:GetRule",
"rbin:ListRules",
"rbin:ListTagsForResource",
"rds:Describe*",
"rds:Download*",
"rds:List*",
"redshift-serverless:GetCustomDomainAssociation",
"redshift-serverless:GetEndpointAccess",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetRecoveryPoint",
"redshift-serverless:GetResourcePolicy",
"redshift-serverless:GetScheduledAction",
"redshift-serverless:GetSnapshot",
"redshift-serverless:GetTableRestoreStatus",
"redshift-serverless:GetUsageLimit",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListCustomDomainAssociations",
"redshift-serverless:ListEndpointAccess",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListRecoveryPoints",
"redshift-serverless:ListScheduledActions",
"redshift-serverless:ListSnapshotCopyConfigurations",
"redshift-serverless:ListSnapshots",
"redshift-serverless:ListTableRestoreStatus",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListUsageLimits",
"redshift-serverless:ListWorkgroups",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"redshift:ListRecommendations",
"redshift:View*",
"refactor-spaces:GetApplication",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetResourcePolicy",
"refactor-spaces:GetRoute",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListEnvironmentVpcs",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
```



```
"refactor-spaces:ListTagsForResource",
"rekognition:CompareFaces",
"rekognition:DescribeDataset",
"rekognition:DescribeProjects",
"rekognition:DescribeProjectVersions",
"rekognition:DescribeStreamProcessor",
"rekognition:Detect*",
"rekognition:GetCelebrityInfo",
"rekognition:GetCelebrityRecognition",
"rekognition:GetContentModeration",
"rekognition:GetFaceDetection",
"rekognition:GetFaceSearch",
"rekognition:GetLabelDetection",
"rekognition:GetPersonTracking",
"rekognition:GetSegmentDetection",
"rekognition:GetTextDetection",
"rekognition:List*",
"rekognition:RecognizeCelebrities",
"rekognition:Search*",
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppAssessment",
"resiliencehub:DescribeAppVersion",
"resiliencehub:DescribeAppVersionAppComponent",
"resiliencehub:DescribeAppVersionResource",
"resiliencehub:DescribeAppVersionResourcesResolutionStatus",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListAlarmRecommendations",
"resiliencehub:ListAppAssessmentComplianceDrifts",
"resiliencehub:ListAppAssessments",
"resiliencehub:ListAppComponentCompliances",
"resiliencehub:ListAppComponentRecommendations",
"resiliencehub:ListAppInputSources",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionAppComponents",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListAppVersionResources",
"resiliencehub:ListAppVersions",
"resiliencehub:ListRecommendationTemplates",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListSopRecommendations",
"resiliencehub:ListSuggestedResiliencyPolicies",
"resiliencehub:ListTagsForResource",
```

```
"resiliencyhub:ListTestRecommendations",
"resiliencyhub: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: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:BatchGetControlEvaluations",
"securityhub:BatchGetSecurityControls",
"securityhub:BatchGetStandardsControlAssociations",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"securitylake:GetDataLakeExceptionSubscription",
"securitylake:GetDataLakeOrganizationConfiguration",
"securitylake:GetDataLakeSources",
"securitylake:GetSubscriber",
"securitylake:ListDataLakeExceptions",
"securitylake:ListDataLakes",
"securitylake:ListLogSources",
"securitylake:ListSubscribers",
"securitylake:ListTagsForResource",
"serverlessrepo:Get*",
"serverlessrepo:List*",
"serverlessrepo:SearchApplications",
"servicecatalog:Describe*",
"servicecatalog:GetApplication",
"servicecatalog:GetAttributeGroup",
"servicecatalog:List*",
"servicecatalog:Scan*",
"servicecatalog:Search*",
"servicediscovery:DiscoverInstances",
"servicediscovery:DiscoverInstancesRevision",
"servicediscovery:Get*",
"servicediscovery:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"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:DescribeOptedOutNumbers",
"sms-voice:DescribeOptOutLists",
"sms-voice:DescribePhoneNumbers",
"sms-voice:DescribePools",
"sms-voice:DescribeSenderId",
"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: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:DescribeCases",
"support:DescribeCommunications",
"support:DescribeServices",
"support:DescribeSeverityLevels",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
"support:DescribeTrustedAdvisorCheckResult",
"support:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"supportplans:GetSupportPlan",
"supportplans:GetSupportPlanUpdateStatus",
"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*",
"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:ListServiceNetworks",
"vpc-lattice:ListServiceNetworkServiceAssociations",
"vpc-lattice:ListServiceNetworkVpcAssociations",
"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:ListAnswers",
"wellarchitected:ListCheckDetails",
"wellarchitected:ListCheckSummaries",
"wellarchitected:ListLenses",
"wellarchitected:ListLensReviewImprovements",
"wellarchitected:ListLensReviews",
"wellarchitected:ListLensShares",
"wellarchitected:ListMilestones",
"wellarchitected:ListNotifications",
"wellarchitected:ListProfileNotifications",
"wellarchitected:ListProfiles",
"wellarchitected:ListProfileShares",
"wellarchitected:ListReviewTemplateAnswers",
"wellarchitected:ListReviewTemplates",
"wellarchitected:ListShareInvitations",
"wellarchitected:ListTagsForResource",
"wellarchitected:ListTemplateShares",
"wellarchitected:ListWorkloads",
"wellarchitected:ListWorkloadShares",
"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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ResourceGroupsandTagEditorFullAccess

描述：提供对 Resource Groups 和标签编辑器的完全访问权限。

ResourceGroupsandTagEditorFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ResourceGroupsandTagEditorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 8 月 10 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ResourceGroupsandTagEditorReadOnlyAccess

描述：提供使用 Resource Groups 和标签编辑器的权限，但不允许通过标签编辑器编辑标签。

ResourceGroupsandTagEditorReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ResourceGroupsandTagEditorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 8 月 10 日 13:42 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ResourceGroupsServiceRolePolicy

描述：允许 AWS Resource Groups 查询拥有您资源的 AWS 服务以保留该组 up-to-date

ResourceGroupsServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 1 月 5 日 16:57 UTC
- 编辑时间：2023 年 1 月 5 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

描述：允许 OpenShift 亚马逊 EBS 容器存储接口 (CSI) 驱动程序操作员在红帽 OpenShift 服务 AWS (ROSA) 集群上安装和维护 Amazon EBS CSI 驱动程序。Amazon EBS CSI 驱动程序允许 ROSA 集群管理 Amazon EBS 持久卷的生命周期。

ROSAAmazonEBSCSIDriverOperatorPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAAmazonEBSCSIDriverOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:36 UTC
- 编辑时间：2023 年 4 月 20 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "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"
        ]
      }
    }
  }
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSACloudNetworkConfigOperatorPolicy

描述：允许 OpenShift Cloud Network Config Config 控制器操作员配置和管理网络资源，供红帽 OpenShift 服务 AWS (ROSA) 集群网络覆盖层使用。OpenShift 云网络运营商通过代表网络插件与 AWS API 交互 CustomResourceDefinitions。Operator 使用这些策略权限来管理作为 ROSA 集群一部分的 Amazon EC2 实例的私有 IP 地址。

ROSACloudNetworkConfigOperatorPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSACloudNetworkConfigOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:34 UTC
- 编辑时间：2023 年 4 月 20 日 22:34 UTC

- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  ]  
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAControlPlaneOperatorPolicy

描述：允许 AWS (ROSA) 控制平面上的红帽 OpenShift 服务管理 ROSA 集群 Amazon EC2 和 Amazon Route 53 资源。

ROSAControlPlaneOperatorPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAControlPlaneOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 24 日 23:02 UTC
- 编辑时间：2023 年 6 月 30 日 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAImageRegistryOperatorPolicy

描述：允许 OpenShift 映像注册操作员配置和管理 Amazon S3 存储桶和对象，供红帽 OpenShift 服务在 AWS (ROSA) 集群内映像注册表上使用，以满足 ROSA 存储要求。OpenShift 映像注册管理器安装和维护红帽 OpenShift 集群的内部注册表。

ROSAImageRegistryOperatorPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAImageRegistryOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:13 UTC

- 编辑时间：世界标准时间 2023 年 12 月 12 日 19:53
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-${aws:RequestedRegion}"
  ]
},
{
  "Sid" : "AllowSpecificObjectActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:ListMultipartUploadParts",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/**",
    "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
  ]
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAIngressOperatorPolicy

描述：允许 OpenShift 入口运营商为集群上的红帽 OpenShift 服务 (ROSA) 配置和管理负载均衡器和域名系统 AWS (DNS) 配置。此策略允许读取标签值，Operator 会筛选标签值以查找 Route 53 资源，发现托管区。

ROSAIngressOperatorPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAIngressOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:37 UTC
- 编辑时间：2023 年 4 月 20 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAInstallerPolicy

描述：允许红帽 OpenShift 服务 AWS (ROSA) 安装程序管理支持 ROSA 群集安装的 AWS 资源。这包括管理 ROSA Worker 节点的实例配置文件。

ROSAInstallerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAInstallerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 6 日 21:00 UTC
- 编辑时间：世界标准时间 2024 年 4 月 24 日 19:49
- ARN: arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAKMSProviderPolicy

描述：允许内置的 ROSA AWS 加密提供商使用客户提供 AWS 的 KMS 密 AWS 钥管理服务 (KMS) 密钥来支持 etcd 数据加密。此策略允许使用 KMS 密钥对数据进行加密和解密。

ROSAKMSProviderPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAKMSProviderPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:10 UTC
- 编辑时间：2023 年 4 月 27 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat" : "true"
        }
    }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAKubeControllerPolicy

描述：允许 ROSA Kubernetes 控制器管理 ROSA 集群的 Amazon EC2、Elastic Load Balancing (ELB) 和 AWS 密钥管理服务 (KMS) 资源。

ROSAKubeControllerPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAKubeControllerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:09 UTC
- 编辑时间：2023 年 10 月 16 日 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "LoadBalancerManagement",
    "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" : "LoadBalancerManagementResourceTag",
    "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"
    }
  }
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAManageSubscription

描述：此策略提供管理红帽 OpenShift 服务 AWS (ROSA) 订阅所需的权限。

ROSAManageSubscription是一个[AWS 托管策略](#)。

使用此策略

您可以将 ROSAManageSubscription 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 11 日 20:58 UTC
- 编辑时间：2023 年 8 月 4 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSANodePoolManagementPolicy

描述：允许红帽 OpenShift 服务 AWS (ROSA) 将集群 EC2 实例作为工作节点进行管理，包括配置安全组以及标记实例和卷的权限。该策略还允许使用 AWS 密钥管理服务 (KMS) 密钥提供的磁盘加密的 EC2 实例。

ROSANodePoolManagementPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSANodePoolManagementPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 8 日 20:48 UTC
- 编辑时间：世界标准时间 2024 年 5 月 2 日 14:01
- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances"
        ]
      }
    }
  }
}
```

```
    }
  },
  {
    "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"
    }
  }
}
]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSASRESupportPolicy

描述：为 ROSA 站点可靠性工程 (SRE) 提供最初观察、诊断和支持 (ROSA) 集群上与红帽 OpenShift 服务 AWS (ROSA) 相关的 AWS 资源所需的权限，包括更改 ROSA 群集节点状态的能力。

ROSASRESupportPolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSASRESupportPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 1 日 14:36 UTC
- 编辑时间：世界标准时间 2024 年 4 月 10 日 20:51
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "DescribeIAMRoles",
  "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"
      }
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ROSAWorkerInstancePolicy

描述：允许您账户中 AWS (ROSA) 工作节点上的红帽 OpenShift 服务对 Amazon EC2 实例和 AWS 区域 计算节点生命周期管理具有只读访问权限。

ROSAWorkerInstancePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ROSAWorkerInstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:35 UTC
- 编辑时间：2023 年 4 月 20 日 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Route53RecoveryReadinessServiceRolePolicy

描述：Route 53 恢复就绪状态的服务关联角色策略

Route53RecoveryReadinessServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2021 年 7 月 15 日 16:06 UTC
- 编辑时间：2023 年 2 月 14 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

Route53ResolverServiceRolePolicy

描述：允许访问 Route53 Resolver AWS 服务 及其使用或管理的资源

Route53ResolverServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 12 日 17:47 UTC
- 编辑时间：2020 年 8 月 12 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```



```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

S3StorageLensServiceRolePolicy

描述：允许访问 S3 Storage Lens AWS 服务 及其使用或管理的资源

S3StorageLensServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 18 日 18:15 UTC
- 编辑时间：2020 年 11 月 18 日 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AwsOrgsAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SecretsManagerReadWrite

描述：通过提供对 S AWS ecrets Manager 的读/写访问权限。AWS Management Console注意：这不包括 IAM 操作，因此FullAccess 如果需要轮换配置，请与 IAM 结合使用。

SecretsManagerReadWrite是一个[AWS 托管策略](#)。

使用此策略

您可以将 SecretsManagerReadWrite 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 18:05 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 18:12

- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
  ]
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SecurityAudit

描述：安全审计模板授予读取安全配置元数据的权限。它对审核 AWS 账户配置的软件非常有用。

SecurityAudit是一个[AWS 托管策略](#)。

使用此策略

您可以将 SecurityAudit 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 4 月 5 日 17:32
- ARN: arn:aws:iam::aws:policy/SecurityAudit

策略版本

策略版本：v42 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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:ListAssessmentFrameworkShareRequests",
"auditmanager:ListAssessmentFrameworks",
"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*",
"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",
"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:ListInstanceStorageConfigs",
"connect:ListInstances",
"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:DescribeImageTags",
"ecr-public:DescribeImages",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImageScanFindings",
"ecr:DescribeImages",
```

```
"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",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeMountTargets",
"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",
"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:GetDataCatalogEncryptionSettings",
"glue:GetDatabases",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTags",
"grafana:ListWorkspaces",
"greengrass:List*",
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
```

```
"health:DescribeAffectedAccountsForOrganization",
"health:DescribeAffectedEntities",
"health:DescribeAffectedEntitiesForOrganization",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
"health:DescribeEventDetails",
"health:DescribeEventDetailsForOrganization",
"health:DescribeEventTypes",
"health:DescribeEvents",
"health:DescribeEventsForOrganization",
"health:DescribeHealthServiceStatusForOrganization",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"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",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"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:GetDiskSnapshots",
"lightsail:GetDisks",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"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*",
"personalize:DescribeDatasetGroup",
"personalize:ListDatasetGroups",
"private-networks:ListNetworks",
"profile:GetDomain",
"profile:ListDomains",
"profile:ListIntegrations",
"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:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListMultiRegionAccessPoints",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemaVersions",
"schemas:ListSchemas",
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
```

```
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecretVersionIds",
"secretsmanager:ListSecrets",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"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:ListQueueTags",
"sqs:ListQueues",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:GetServiceSetting",
"ssm:ListAssociationVersions",
"ssm:ListAssociations",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocumentVersions",
"ssm:ListDocuments",
"ssm:ListInventoryEntries",
"ssm:ListOpsMetadata",
"ssm:ListResourceComplianceSummaries",
"ssm:ListResourceDataSync",
"ssm:ListTagsForResource",
"sso:DescribeAccountAssignmentCreationStatus",
"sso:DescribePermissionSet",
"sso:DescribePermissionsPolicies",
"sso:List*",
"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:DescribeTrustedAdvisorCheckSummaries",
"support:DescribeTrustedAdvisorChecks",
"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"
]
}
]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SecurityLakeServiceLinkedRole

描述：本政策授予代表您操作亚马逊安全湖服务的权限

SecurityLakeServiceLinkedRole是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 29 日 14:03 UTC
- 编辑时间：世界标准时间 2024 年 4 月 19 日 16:00
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigration_ServiceRole

描述：允许 AWS 服务器迁移服务将虚拟机迁移到 EC2 的权限：允许服务器迁移服务将迁移的资源存入客户的 EC2 账户。

ServerMigration_ServiceRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServerMigration_ServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 11 日 20:41 UTC
- 编辑时间：2020 年 10 月 15 日 17:26 UTC

- ARN: arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigrationConnector

描述：允许 AWS 服务器迁移连接器将虚拟机迁移到 EC2 的权限。允许与 AWS 服务器迁移服务通信、对以 'sms-b-' 和 'import-to-ec2-' 开头的 S3 存储桶以及用于 AWS 服务器迁移连接器升级、AWS 服务器迁移连接器注册和指标上传到的存储桶的读/写访问权限。AWS AWS

ServerMigrationConnector 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServerMigrationConnector 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 10 月 24 日 21:45 UTC
- 编辑时间：2016 年 10 月 24 日 21:45 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationConnector

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigrationServiceConsoleFullAccess

描述：使用服务器迁移服务控制台所有功能所需的权限

ServerMigrationServiceConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServerMigrationServiceConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 9 日 17:18 UTC
- 编辑时间：2020 年 7 月 20 日 22:00 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigrationServiceLaunchRole

描述：允许 AWS 服务器迁移服务创建相关 AWS 资源并将其更新到客户的资源中以启动迁移 AWS 账户的服务器和应用程序的权限。

ServerMigrationServiceLaunchRole 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServerMigrationServiceLaunchRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 26 日 19:53 UTC
- 编辑时间：2020 年 10 月 15 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigrationServiceRoleForInstanceValidation

描述：允许 SMS 运行使用的数据验证脚本并将脚本成功/失败发送回 AWS 短信的权限

ServerMigrationServiceRoleForInstanceValidation 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServerMigrationServiceRoleForInstanceValidation 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 7 月 20 日 22:25 UTC
- 编辑时间：2020 年 7 月 20 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServiceQuotasFullAccess

描述：提供对 Service Quotas 的完全访问权限

ServiceQuotasFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `ServiceQuotasFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 24 日 15:44 UTC
- 编辑时间：2021 年 2 月 4 日 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServiceQuotasReadOnlyAccess

描述：提供对 Service Quotas 的只读访问权限

ServiceQuotasReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ServiceQuotasReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 24 日 15:31 UTC
- 编辑时间：2020 年 12 月 21 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServiceQuotasServiceRolePolicy

描述：允许 Service Quotas 代表你创建支持案例

ServiceQuotasServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 5 月 22 日 20:44 UTC
- 编辑时间：2019 年 6 月 24 日 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Action" : [
    "support:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SimpleWorkflowFullAccess

描述：提供对简单 workflow 配置服务的完全访问权限。

SimpleWorkflowFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 SimpleWorkflowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/SimpleWorkflowFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SplitCostAllocationDataServiceRolePolicy

描述：允许拆分成本分配数据检索 AWS Organizations 信息（如果适用），并收集客户选择加入的分割成本分配数据服务的遥测数据。

SplitCostAllocationDataServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 4 月 16 日 16:05
- 编辑时间：世界标准时间 2024 年 4 月 16 日 16:05

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

SupportUser

描述：此策略授予对中问题进行故障排除和解决的权限 AWS 账户。该政策还允许用户联系 AWS 支持人员以创建和管理案例。

SupportUser 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 SupportUser 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:21 UTC
- 编辑时间：2023 年 8 月 25 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SystemAdministrator

描述：授予应用程序和开发操作所需资源所需的完全访问权限。

SystemAdministrator是一个[AWS 托管策略](#)。

使用此策略

您可以将 SystemAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:23 UTC
- 编辑时间：2020 年 8 月 24 日 20:05 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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: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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

TranslateFullAccess

描述：提供对 Amazon Translate 的完全访问权限。

TranslateFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 TranslateFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 23:36 UTC

- 编辑时间：2020 年 1 月 8 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

TranslateReadOnly

描述：提供对 Amazon Translate 的只读访问权限。

TranslateReadOnly是一个[AWS 托管策略](#)。

使用此策略

您可以将 TranslateReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 18:22 UTC
- 编辑时间：2023 年 5 月 24 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/TranslateReadOnly

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ViewOnlyAccess

描述：此策略授予查看所有 AWS 服务的资源和基本元数据的权限。

ViewOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 ViewOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:20 UTC
- 编辑时间：世界标准时间 2024 年 6 月 10 日 20:57
- ARN: arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

策略版本

策略版本：v19 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "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:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupPlans",
        "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:BatchGetDeploymentTargets",
"codedeploy:BatchGetDeployments",
"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:ListRecommendationSummaries",
"cost-optimization-hub:ListRecommendations",
"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:DescribeIdFormat",
"ec2:DescribeIdentityIdFormat",
"ec2:DescribeImage*",
"ec2:DescribeImport*",
"ec2:DescribeInstance*",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeLocalGatewayRouteTables",
"ec2:DescribeLocalGatewayVirtualInterfaceGroups",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeLocalGateways",
"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",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAcceleratorTypes",
```

```
"elastic-inference:DescribeAccelerators",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeEnvironments",
"elasticbeanstalk:ListAvailableSolutionStacks",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"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:GetBotVersions",
"lex:GetBots",
"lex:GetIntentVersions",
"lex:GetIntents",
"lex:GetSlotTypeVersions",
"lex:GetSlotTypes",
"lex:GetUtterancesView",
"lightsail:GetBlueprints",
"lightsail:GetBundles",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetRegions",
"lightsail:GetStaticIps",
"lightsail:IsVpcPeered",
"logs:Describe*",
"logs:ListTagsForResource",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"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",
"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:ListQueueTags",
"sqs:ListQueues",
"ssm:ListAssociations",
"ssm:ListDocuments",
"states:ListActivities",
"states:ListStateMachineAliases",
"states:ListStateMachineVersions",
"states:ListStateMachines",
"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"
  ]
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

VMImportExportRoleForAWSConnector

描述：虚拟机导入/导出服务角色的默认策略，适用于使用连接器的客户。AWS 虚拟机导入/导出服务扮演此策略的角色，以满足来自 Conn AWS ector 虚拟设备的虚拟机迁移请求。（请注意，AWS 连接器使用“AWSConnector”托管策略代表客户向虚拟机导入/导出服务发出请求。）提供创建 AMI 和 EBS 快照、修改 EBS 快照属性、对 EC2 对象进行“描述*”调用以及从以 '2-' 开头的 S3 存储桶读取数据的功能。import-to-ec

VMImportExportRoleForAWSConnector 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 `VMImportExportRoleForAWSConnector` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 9 月 3 日 20:48 UTC
- 编辑时间：2015 年 9 月 3 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

VPCLatticeFullAccess

描述：提供对 Amazon VPC Lattice 的完全访问权限和对依赖服务的访问权限。

VPCLatticeFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 VPCLatticeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:49 UTC
- 编辑时间：2023 年 3 月 30 日 02:49 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ],
      "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"
  }
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

VPCLatticeReadOnlyAccess

描述：通过提供对 Amazon VPC Lattice 的只读访问权限 AWS Management Console，以及对依赖服务的有限访问权限。

VPCLatticeReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 VPCLatticeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:47 UTC
- 编辑时间：2023 年 3 月 30 日 02:47 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

VPCLatticeServicesInvokeAccess

描述：提供调用 Amazon VPC 莱迪思服务的权限。

VPCLatticeServicesInvokeAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 VPCLatticeServicesInvokeAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:45 UTC
- 编辑时间：2023 年 3 月 30 日 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

WAFLoggingServiceRolePolicy

描述：创建 SLR 以将客户的日志写入火管流

WAFLoggingServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 24 日 21:05 UTC
- 编辑时间：2018 年 8 月 24 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

WAFRegionalLoggingServiceRolePolicy

描述：创建 SLR 以将客户的日志写入火管流

WAFRegionalLoggingServiceRolePolicy是一个[AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 24 日 18:40 UTC
- 编辑时间：2018 年 8 月 24 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

WAFV2LoggingServiceRolePolicy

描述：此策略创建了一个服务相关角色，允许 AWS WAF 向 Amazon Kinesis Data Firehose 写入日志。

WAFV2LoggingServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 7 日 00:40 UTC
- 编辑时间：世界标准时间 2024 年 6 月 3 日 17:29
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

WellArchitectedConsoleFullAccess

描述：提供通过 Well-Architect AWS ed 工具的完整访问权限 AWS Management Console

WellArchitectedConsoleFullAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 WellArchitectedConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 18:19 UTC
- 编辑时间：2018 年 11 月 29 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

WellArchitectedConsoleReadOnlyAccess

描述：通过 Well-Architect AWS ed 工具提供只读访问权限 AWS Management Console

WellArchitectedConsoleReadOnlyAccess 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 WellArchitectedConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 18:21 UTC
- 编辑时间：2023 年 6 月 29 日 17:16 UTC
- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

WorkLinkServiceRolePolicy

描述：允许访问 Amazon AWS 服务 及其使用或管理的资源 WorkLink

WorkLinkServiceRolePolicy 是一个 [AWS 托管策略](#)。

使用此策略

您可以将 WorkLinkServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 23 日 19:03 UTC
- 编辑时间：2019 年 1 月 23 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。