



Guia de referência

# AWS Política gerenciada



# AWS Política gerenciada: Guia de referência

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

# Table of Contents

O que são as políticas gerenciadas pela AWS? .....	1
Compreender as páginas de referência de políticas .....	1
Políticas gerenciadas pela AWS obsoletas .....	2
AWS políticas gerenciadas .....	3
AccessAnalyzerServiceRolePolicy .....	43
Utilização desta política .....	43
Detalhes desta política .....	43
Versão da política .....	43
Documento da política JSON .....	44
Saiba mais .....	46
AdministratorAccess .....	46
Utilização desta política .....	46
Detalhes desta política .....	46
Versão da política .....	46
Documento da política JSON .....	47
Saiba mais .....	47
AdministratorAccess-Amplify .....	47
A utilização desta política .....	47
Detalhes da política .....	47
Versão da política .....	48
Documento da política JSON .....	48
Saiba mais .....	58
AdministratorAccess-AWSElasticBeanstalk .....	58
A utilização desta política .....	59
Detalhes da política .....	59
Versão da política .....	59
Documento da política JSON .....	59
Saiba mais .....	67
AlexaForBusinessDeviceSetup .....	68
A utilização desta política .....	68
Detalhes da política .....	68
Versão da política .....	68
Documento da política JSON .....	68
Saiba mais .....	69

AlexaForBusinessFullAccess .....	69
A utilização desta política .....	69
Detalhes da política .....	69
Versão da política .....	70
Documento da política JSON .....	70
Saiba mais .....	71
AlexaForBusinessGatewayExecution .....	71
A utilização desta política .....	71
Detalhes da política .....	72
Versão da política .....	72
Documento da política JSON .....	72
Saiba mais .....	73
AlexaForBusinessLifesizeDelegatedAccessPolicy .....	73
A utilização desta política .....	73
Detalhes da política .....	73
Versão da política .....	74
Documento da política JSON .....	74
Saiba mais .....	76
AlexaForBusinessNetworkProfileServicePolicy .....	76
A utilização desta política .....	76
Detalhes da política .....	76
Versão da política .....	77
Documento da política JSON .....	77
Saiba mais .....	78
AlexaForBusinessPolyDelegatedAccessPolicy .....	78
A utilização desta política .....	78
Detalhes da política .....	78
Versão da política .....	78
Documento da política JSON .....	78
Saiba mais .....	80
AlexaForBusinessReadOnlyAccess .....	80
A utilização desta política .....	81
Detalhes da política .....	81
Versão da política .....	81
Documento da política JSON .....	81
Saiba mais .....	81

AmazonAPIGatewayAdministrator .....	82
A utilização desta política .....	82
Detalhes da política .....	82
Versão da política .....	82
Documento da política JSON .....	82
Saiba mais .....	83
AmazonAPIGatewayInvokeFullAccess .....	83
A utilização desta política .....	83
Detalhes da política .....	83
Versão da política .....	83
Documento da política JSON .....	84
Saiba mais .....	84
AmazonAPIGatewayPushToCloudWatchLogs .....	84
A utilização desta política .....	84
Detalhes da política .....	84
Versão da política .....	85
Documento da política JSON .....	85
Saiba mais .....	85
AmazonAppFlowFullAccess .....	86
A utilização desta política .....	86
Detalhes da política .....	86
Versão da política .....	86
Documento da política JSON .....	86
Saiba mais .....	89
AmazonAppFlowReadOnlyAccess .....	89
A utilização desta política .....	89
Detalhes da política .....	89
Versão da política .....	90
Documento da política JSON .....	90
Saiba mais .....	90
AmazonAppStreamFullAccess .....	91
A utilização desta política .....	91
Detalhes da política .....	91
Versão da política .....	91
Documento da política JSON .....	91
Saiba mais .....	93

AmazonAppStreamPCAAccess .....	93
A utilização desta política .....	93
Detalhes da política .....	94
Versão da política .....	94
Documento da política JSON .....	94
Saiba mais .....	94
AmazonAppStreamReadOnlyAccess .....	95
A utilização desta política .....	95
Detalhes da política .....	95
Versão da política .....	95
Documento da política JSON .....	95
Saiba mais .....	96
AmazonAppStreamServiceAccess .....	96
A utilização desta política .....	96
Detalhes da política .....	96
Versão da política .....	96
Documento da política JSON .....	97
Saiba mais .....	98
AmazonAthenaFullAccess .....	98
Utilização desta política .....	98
Detalhes desta política .....	98
Versão da política .....	98
Documento da política JSON .....	99
Saiba mais .....	102
AmazonAugmentedAIFullAccess .....	102
A utilização desta política .....	102
Detalhes da política .....	103
Versão da política .....	103
Documento da política JSON .....	103
Saiba mais .....	104
AmazonAugmentedAIHumanLoopFullAccess .....	104
A utilização desta política .....	104
Detalhes da política .....	104
Versão da política .....	105
Documento da política JSON .....	105
Saiba mais .....	105

AmazonAugmentedAllIntegratedAPIAccess .....	106
A utilização desta política .....	106
Detalhes da política .....	106
Versão da política .....	106
Documento da política JSON .....	106
Saiba mais .....	108
AmazonBedrockFullAccess .....	108
Utilização desta política .....	108
Detalhes desta política .....	108
Versão da política .....	108
Documento da política JSON .....	108
Saiba mais .....	110
AmazonBedrockReadOnly .....	110
Utilização desta política .....	110
Detalhes desta política .....	110
Versão da política .....	110
Documento da política JSON .....	111
Saiba mais .....	111
AmazonBraketFullAccess .....	112
A utilização desta política .....	112
Detalhes da política .....	112
Versão da política .....	112
Documento da política JSON .....	112
Saiba mais .....	116
AmazonBraketJobsExecutionPolicy .....	117
A utilização desta política .....	117
Detalhes da política .....	117
Versão da política .....	117
Documento da política JSON .....	117
Saiba mais .....	120
AmazonBraketServiceRolePolicy .....	120
A utilização desta política .....	120
Detalhes da política .....	120
Versão da política .....	120
Documento da política JSON .....	121
Saiba mais .....	121

AmazonChimeFullAccess .....	122
A utilização desta política .....	122
Detalhes da política .....	122
Versão da política .....	122
Documento da política JSON .....	122
Saiba mais .....	124
AmazonChimeReadOnly .....	125
A utilização desta política .....	125
Detalhes da política .....	125
Versão da política .....	125
Documento da política JSON .....	125
Saiba mais .....	126
AmazonChimeSDK .....	126
A utilização desta política .....	126
Detalhes da política .....	126
Versão da política .....	126
Documento da política JSON .....	127
Saiba mais .....	128
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy .....	128
A utilização desta política .....	128
Detalhes desta política .....	128
Versão da política .....	128
Documento da política JSON .....	129
Saiba mais .....	130
AmazonChimeSDKMessagingServiceRolePolicy .....	130
A utilização desta política .....	130
Detalhes da política .....	130
Versão da política .....	130
Documento da política JSON .....	131
Saiba mais .....	131
AmazonChimeServiceRolePolicy .....	132
A utilização desta política .....	132
Detalhes da política .....	132
Versão da política .....	132
Documento da política JSON .....	132
Saiba mais .....	133



AmazonChimeTranscriptionServiceLinkedRolePolicy .....	133
A utilização desta política .....	133
Detalhes da política .....	133
Versão da política .....	133
Documento da política JSON .....	134
Saiba mais .....	134
AmazonChimeUserManagement .....	134
A utilização desta política .....	134
Detalhes da política .....	134
Versão da política .....	135
Documento da política JSON .....	135
Saiba mais .....	136
AmazonChimeVoiceConnectorServiceLinkedRolePolicy .....	136
A utilização desta política .....	136
Detalhes da política .....	137
Versão da política .....	137
Documento da política JSON .....	137
Saiba mais .....	139
AmazonCloudDirectoryFullAccess .....	139
A utilização desta política .....	139
Detalhes da política .....	139
Versão da política .....	139
Documento da política JSON .....	140
Saiba mais .....	140
AmazonCloudDirectoryReadOnlyAccess .....	140
A utilização desta política .....	140
Detalhes da política .....	140
Versão da política .....	141
Documento da política JSON .....	141
Saiba mais .....	141
AmazonCloudWatchEvidentlyFullAccess .....	142
A utilização desta política .....	142
Detalhes da política .....	142
Versão da política .....	142
Documento da política JSON .....	142
Saiba mais .....	145

AmazonCloudWatchEvidentlyReadOnlyAccess .....	145
A utilização desta política .....	145
Detalhes da política .....	145
Versão da política .....	145
Documento da política JSON .....	146
Saiba mais .....	146
AmazonCloudWatchEvidentlyServiceRolePolicy .....	146
A utilização desta política .....	147
Detalhes da política .....	147
Versão da política .....	147
Documento da política JSON .....	147
Saiba mais .....	149
AmazonCloudWatchRUMFullAccess .....	149
A utilização desta política .....	149
Detalhes da política .....	149
Versão da política .....	149
Documento da política JSON .....	149
Saiba mais .....	152
AmazonCloudWatchRUMReadOnlyAccess .....	152
A utilização desta política .....	152
Detalhes da política .....	152
Versão da política .....	153
Documento da política JSON .....	153
Saiba mais .....	153
AmazonCloudWatchRUMServiceRolePolicy .....	154
A utilização desta política .....	154
Detalhes da política .....	154
Versão da política .....	154
Documento da política JSON .....	154
Saiba mais .....	155
AmazonCodeCatalystFullAccess .....	155
A utilização desta política .....	155
Detalhes da política .....	155
Versão da política .....	156
Documento da política JSON .....	156
Saiba mais .....	157

AmazonCodeCatalystReadOnlyAccess .....	157
A utilização desta política .....	157
Detalhes da política .....	157
Versão da política .....	157
Documento da política JSON .....	157
Saiba mais .....	158
AmazonCodeCatalystSupportAccess .....	158
A utilização desta política .....	158
Detalhes da política .....	158
Versão da política .....	159
Documento da política JSON .....	159
Saiba mais .....	159
AmazonCodeGuruProfilerAgentAccess .....	160
A utilização desta política .....	160
Detalhes da política .....	160
Versão da política .....	160
Documento da política JSON .....	160
Saiba mais .....	161
AmazonCodeGuruProfilerFullAccess .....	161
A utilização desta política .....	161
Detalhes da política .....	161
Versão da política .....	161
Documento da política JSON .....	162
Saiba mais .....	162
AmazonCodeGuruProfilerReadOnlyAccess .....	163
A utilização desta política .....	163
Detalhes da política .....	163
Versão da política .....	163
Documento da política JSON .....	163
Saiba mais .....	164
AmazonCodeGuruReviewerFullAccess .....	164
A utilização desta política .....	164
Detalhes da política .....	164
Versão da política .....	164
Documento da política JSON .....	165
Saiba mais .....	167

AmazonCodeGuruReviewerReadOnlyAccess .....	167
A utilização desta política .....	168
Detalhes da política .....	168
Versão da política .....	168
Documento da política JSON .....	168
Saiba mais .....	169
AmazonCodeGuruReviewerServiceRolePolicy .....	169
A utilização desta política .....	169
Detalhes da política .....	169
Versão da política .....	169
Documento da política JSON .....	170
Saiba mais .....	172
AmazonCodeGuruSecurityFullAccess .....	172
A utilização desta política .....	172
Detalhes da política .....	172
Versão da política .....	172
Documento da política JSON .....	172
Saiba mais .....	173
AmazonCodeGuruSecurityScanAccess .....	173
A utilização desta política .....	173
Detalhes da política .....	173
Versão da política .....	173
Documento da política JSON .....	174
Saiba mais .....	174
AmazonCognitoDeveloperAuthenticatedIdentities .....	174
A utilização desta política .....	175
Detalhes da política .....	175
Versão da política .....	175
Documento da política JSON .....	175
Saiba mais .....	176
AmazonCognitoIdpEmailServiceRolePolicy .....	176
A utilização desta política .....	176
Detalhes da política .....	176
Versão da política .....	176
Documento da política JSON .....	177
Saiba mais .....	177

AmazonCognitoDpServiceRolePolicy .....	177
A utilização desta política .....	177
Detalhes da política .....	178
Versão da política .....	178
Documento da política JSON .....	178
Saiba mais .....	178
AmazonCognitoPowerUser .....	179
A utilização desta política .....	179
Detalhes da política .....	179
Versão da política .....	179
Documento da política JSON .....	179
Saiba mais .....	181
AmazonCognitoReadOnly .....	181
A utilização desta política .....	181
Detalhes da política .....	181
Versão da política .....	181
Documento da política JSON .....	181
Saiba mais .....	182
AmazonCognitoUnAuthedIdentitiesSessionPolicy .....	182
A utilização desta política .....	183
Detalhes da política .....	183
Versão da política .....	183
Documento da política JSON .....	183
Saiba mais .....	184
AmazonCognitoUnauthenticatedIdentities .....	184
A utilização desta política .....	184
Detalhes da política .....	184
Versão da política .....	185
Documento da política JSON .....	185
Saiba mais .....	185
AmazonConnect_FullAccess .....	185
A utilização desta política .....	186
Detalhes da política .....	186
Versão da política .....	186
Documento da política JSON .....	186
Saiba mais .....	189

AmazonConnectCampaignsServiceLinkedRolePolicy .....	189
Utilização desta política .....	189
Detalhes desta política .....	189
Versão da política .....	189
Documento da política JSON .....	190
Saiba mais .....	190
AmazonConnectReadOnlyAccess .....	190
A utilização desta política .....	191
Detalhes da política .....	191
Versão da política .....	191
Documento da política JSON .....	191
Saiba mais .....	192
AmazonConnectServiceLinkedRolePolicy .....	192
Utilização desta política .....	192
Detalhes desta política .....	192
Versão da política .....	192
Documento da política JSON .....	193
Saiba mais .....	197
AmazonConnectSynchronizationServiceRolePolicy .....	197
A utilização desta política .....	198
Detalhes da política .....	198
Versão da política .....	198
Documento da política JSON .....	198
Saiba mais .....	200
AmazonConnectVoiceIDFullAccess .....	200
A utilização desta política .....	200
Detalhes da política .....	200
Versão da política .....	201
Documento da política JSON .....	201
Saiba mais .....	201
AmazonDataZoneDomainExecutionRolePolicy .....	201
Utilização desta política .....	202
Detalhes desta política .....	202
Versão da política .....	202
Documento da política JSON .....	202
Saiba mais .....	205

AmazonDataZoneEnvironmentRolePermissionsBoundary .....	205
Utilização desta política .....	205
Detalhes desta política .....	205
Versão da política .....	206
Documento da política JSON .....	206
Saiba mais .....	219
AmazonDataZoneFullAccess .....	219
Utilização desta política .....	219
Detalhes desta política .....	219
Versão da política .....	219
Documento da política JSON .....	220
Saiba mais .....	223
AmazonDataZoneFullUserAccess .....	223
Utilização desta política .....	223
Detalhes desta política .....	223
Versão da política .....	223
Documento da política JSON .....	224
Saiba mais .....	226
AmazonDataZoneGlueManageAccessRolePolicy .....	227
Utilização desta política .....	227
Detalhes desta política .....	227
Versão da política .....	227
Documento da política JSON .....	227
Saiba mais .....	231
AmazonDataZonePortalFullAccessPolicy .....	231
A utilização desta política .....	231
Detalhes da política .....	231
Versão da política .....	232
Documento da política JSON .....	232
Saiba mais .....	232
AmazonDataZonePreviewConsoleFullAccess .....	232
A utilização desta política .....	232
Detalhes da política .....	233
Versão da política .....	233
Documento da política JSON .....	233
Saiba mais .....	235

AmazonDataZoneProjectDeploymentPermissionsBoundary .....	235
A utilização desta política .....	235
Detalhes da política .....	235
Versão da política .....	236
Documento da política JSON .....	236
Saiba mais .....	244
AmazonDataZoneProjectRolePermissionsBoundary .....	244
A utilização desta política .....	244
Detalhes da política .....	244
Versão da política .....	244
Documento da política JSON .....	245
Saiba mais .....	252
AmazonDataZoneRedshiftGlueProvisioningPolicy .....	252
Utilização desta política .....	252
Detalhes desta política .....	252
Versão da política .....	253
Documento da política JSON .....	253
Saiba mais .....	260
AmazonDataZoneRedshiftManageAccessRolePolicy .....	261
Utilização desta política .....	261
Detalhes desta política .....	261
Versão da política .....	261
Documento da política JSON .....	261
Saiba mais .....	264
AmazonDetectiveFullAccess .....	264
A utilização desta política .....	264
Detalhes da política .....	264
Versão da política .....	264
Documento da política JSON .....	264
Saiba mais .....	265
AmazonDetectiveInvestigatorAccess .....	266
Utilização desta política .....	266
Detalhes desta política .....	266
Versão da política .....	266
Documento da política JSON .....	266
Saiba mais .....	268



AmazonDetectiveMemberAccess .....	268
A utilização desta política .....	268
Detalhes da política .....	268
Versão da política .....	268
Documento da política JSON .....	269
Saiba mais .....	269
AmazonDetectiveOrganizationsAccess .....	269
A utilização desta política .....	270
Detalhes da política .....	270
Versão da política .....	270
Documento da política JSON .....	270
Saiba mais .....	272
AmazonDetectiveServiceLinkedRolePolicy .....	272
A utilização desta política .....	272
Detalhes da política .....	272
Versão da política .....	273
Documento da política JSON .....	273
Saiba mais .....	273
AmazonDevOpsGuruConsoleFullAccess .....	273
A utilização desta política .....	273
Detalhes da política .....	274
Versão da política .....	274
Documento da política JSON .....	274
Saiba mais .....	276
AmazonDevOpsGuruFullAccess .....	277
A utilização desta política .....	277
Detalhes da política .....	277
Versão da política .....	277
Documento da política JSON .....	277
Saiba mais .....	279
AmazonDevOpsGuruOrganizationsAccess .....	280
A utilização desta política .....	280
Detalhes da política .....	280
Versão da política .....	280
Documento da política JSON .....	280
Saiba mais .....	282

AmazonDevOpsGuruReadOnlyAccess .....	282
A utilização desta política .....	282
Detalhes da política .....	282
Versão da política .....	282
Documento da política JSON .....	282
Saiba mais .....	284
AmazonDevOpsGuruServiceRolePolicy .....	285
A utilização desta política .....	285
Detalhes da política .....	285
Versão da política .....	285
Documento da política JSON .....	285
Saiba mais .....	289
AmazonDMSCloudWatchLogsRole .....	289
A utilização desta política .....	290
Detalhes da política .....	290
Versão da política .....	290
Documento da política JSON .....	290
Saiba mais .....	292
AmazonDMSRedshiftS3Role .....	292
A utilização desta política .....	292
Detalhes da política .....	292
Versão da política .....	292
Documento da política JSON .....	292
Saiba mais .....	293
AmazonDMSVPCManagementRole .....	293
A utilização desta política .....	294
Detalhes da política .....	294
Versão da política .....	294
Documento da política JSON .....	294
Saiba mais .....	295
AmazonDocDB-ElasticServiceRolePolicy .....	295
A utilização desta política .....	295
Detalhes da política .....	295
Versão da política .....	295
Documento da política JSON .....	295
Saiba mais .....	296

AmazonDocDBConsoleFullAccess .....	296
A utilização desta política .....	296
Detalhes da política .....	297
Versão da política .....	297
Documento da política JSON .....	297
Saiba mais .....	301
AmazonDocDBElasticFullAccess .....	301
A utilização desta política .....	302
Detalhes da política .....	302
Versão da política .....	302
Documento da política JSON .....	302
Saiba mais .....	305
AmazonDocDBElasticReadOnlyAccess .....	305
A utilização desta política .....	305
Detalhes da política .....	305
Versão da política .....	306
Documento da política JSON .....	306
Saiba mais .....	307
AmazonDocDBFullAccess .....	307
A utilização desta política .....	307
Detalhes da política .....	307
Versão da política .....	307
Documento da política JSON .....	307
Saiba mais .....	310
AmazonDocDBReadOnlyAccess .....	310
A utilização desta política .....	311
Detalhes da política .....	311
Versão da política .....	311
Documento da política JSON .....	311
Saiba mais .....	313
AmazonDRSVPCManagement .....	313
A utilização desta política .....	313
Detalhes da política .....	313
Versão da política .....	314
Documento da política JSON .....	314
Saiba mais .....	314

AmazonDynamoDBFullAccess .....	315
A utilização desta política .....	315
Detalhes da política .....	315
Versão da política .....	315
Documento da política JSON .....	315
Saiba mais .....	318
AmazonDynamoDBFullAccesswithDataPipeline .....	318
A utilização desta política .....	318
Detalhes da política .....	318
Versão da política .....	319
Documento da política JSON .....	319
Saiba mais .....	321
AmazonDynamoDBReadOnlyAccess .....	321
Utilização desta política .....	321
Detalhes desta política .....	321
Versão da política .....	321
Documento da política JSON .....	322
Saiba mais .....	323
AmazonEBSCSIDriverPolicy .....	324
A utilização desta política .....	324
Detalhes da política .....	324
Versão da política .....	324
Documento da política JSON .....	324
Saiba mais .....	327
AmazonEC2ContainerRegistryFullAccess .....	328
A utilização desta política .....	328
Detalhes da política .....	328
Versão da política .....	328
Documento da política JSON .....	328
Saiba mais .....	329
AmazonEC2ContainerRegistryPowerUser .....	329
A utilização desta política .....	329
Detalhes da política .....	329
Versão da política .....	330
Documento da política JSON .....	330
Saiba mais .....	331

---

AmazonEC2ContainerRegistryReadOnly .....	331
A utilização desta política .....	331
Detalhes da política .....	331
Versão da política .....	331
Documento da política JSON .....	331
Saiba mais .....	332
AmazonEC2ContainerServiceAutoscaleRole .....	332
A utilização desta política .....	332
Detalhes da política .....	333
Versão da política .....	333
Documento da política JSON .....	333
Saiba mais .....	334
AmazonEC2ContainerServiceEventsRole .....	334
A utilização desta política .....	334
Detalhes da política .....	334
Versão da política .....	334
Documento da política JSON .....	335
Saiba mais .....	336
AmazonEC2ContainerServiceforEC2Role .....	336
A utilização desta política .....	336
Detalhes da política .....	336
Versão da política .....	336
Documento da política JSON .....	336
Saiba mais .....	337
AmazonEC2ContainerServiceRole .....	338
A utilização desta política .....	338
Detalhes da política .....	338
Versão da política .....	338
Documento da política JSON .....	338
Saiba mais .....	339
AmazonEC2FullAccess .....	339
A utilização desta política .....	339
Detalhes da política .....	339
Versão da política .....	340
Documento da política JSON .....	340
Saiba mais .....	341

AmazonEC2ReadOnlyAccess .....	341
Utilização desta política .....	341
Detalhes desta política .....	341
Versão da política .....	341
Documento da política JSON .....	342
Saiba mais .....	342
AmazonEC2RoleforAWSCodeDeploy .....	343
A utilização desta política .....	343
Detalhes da política .....	343
Versão da política .....	343
Documento da política JSON .....	343
Saiba mais .....	344
AmazonEC2RoleforAWSCodeDeployLimited .....	344
A utilização desta política .....	344
Detalhes da política .....	344
Versão da política .....	344
Documento da política JSON .....	345
Saiba mais .....	345
AmazonEC2RoleforDataPipelineRole .....	346
A utilização desta política .....	346
Detalhes da política .....	346
Versão da política .....	346
Documento da política JSON .....	346
Saiba mais .....	347
AmazonEC2RoleforSSM .....	347
A utilização desta política .....	347
Detalhes da política .....	347
Versão da política .....	348
Documento da política JSON .....	348
Saiba mais .....	350
AmazonEC2RolePolicyForLaunchWizard .....	350
A utilização desta política .....	350
Detalhes da política .....	351
Versão da política .....	351
Documento da política JSON .....	351
Saiba mais .....	355

AmazonEC2SpotFleetAutoscaleRole .....	355
A utilização desta política .....	355
Detalhes da política .....	355
Versão da política .....	356
Documento da política JSON .....	356
Saiba mais .....	357
AmazonEC2SpotFleetTaggingRole .....	357
A utilização desta política .....	357
Detalhes da política .....	357
Versão da política .....	357
Documento da política JSON .....	358
Saiba mais .....	359
AmazonECS_FullAccess .....	359
A utilização desta política .....	359
Detalhes da política .....	359
Versão da política .....	360
Documento da política JSON .....	360
Saiba mais .....	365
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity .....	365
Utilização desta política .....	366
Detalhes desta política .....	366
Versão da política .....	366
Documento da política JSON .....	366
Saiba mais .....	368
AmazonECSInfrastructureRolePolicyForVolumes .....	369
Utilização desta política .....	369
Detalhes desta política .....	369
Versão da política .....	369
Documento da política JSON .....	369
Saiba mais .....	371
AmazonECSServiceRolePolicy .....	371
Utilização desta política .....	372
Detalhes desta política .....	372
Versão da política .....	372
Documento da política JSON .....	372
Saiba mais .....	377

AmazonECSTaskExecutionRolePolicy .....	377
A utilização desta política .....	377
Detalhes da política .....	377
Versão da política .....	377
Documento da política JSON .....	378
Saiba mais .....	378
AmazonEFSCSIDriverPolicy .....	378
A utilização desta política .....	379
Detalhes da política .....	379
Versão da política .....	379
Documento da política JSON .....	379
Saiba mais .....	381
AmazonEKS_CNI_Policy .....	381
Utilização desta política .....	381
Detalhes desta política .....	381
Versão da política .....	381
Documento da política JSON .....	382
Saiba mais .....	382
AmazonEKSClusterPolicy .....	383
A utilização desta política .....	383
Detalhes da política .....	383
Versão da política .....	383
Documento da política JSON .....	383
Saiba mais .....	385
AmazonEKSClusterConnectorServiceRolePolicy .....	386
A utilização desta política .....	386
Detalhes da política .....	386
Versão da política .....	386
Documento da política JSON .....	386
Saiba mais .....	388
AmazonEKSFargatePodExecutionRolePolicy .....	388
A utilização desta política .....	388
Detalhes da política .....	388
Versão da política .....	389
Documento da política JSON .....	389
Saiba mais .....	389



AmazonEKSFargateServiceRolePolicy .....	390
A utilização desta política .....	390
Detalhes da política .....	390
Versão da política .....	390
Documento da política JSON .....	390
Saiba mais .....	391
AmazonEKSLocalOutpostClusterPolicy .....	391
A utilização desta política .....	391
Detalhes da política .....	391
Versão da política .....	391
Documento da política JSON .....	392
Saiba mais .....	393
AmazonEKSLocalOutpostServiceRolePolicy .....	394
A utilização desta política .....	394
Detalhes da política .....	394
Versão da política .....	394
Documento da política JSON .....	394
Saiba mais .....	400
AmazonEKSServicePolicy .....	400
A utilização desta política .....	400
Detalhes da política .....	400
Versão da política .....	401
Documento da política JSON .....	401
Saiba mais .....	402
AmazonEKSServiceRolePolicy .....	403
A utilização desta política .....	403
Detalhes da política .....	403
Versão da política .....	403
Documento da política JSON .....	403
Saiba mais .....	405
AmazonEKSVPCResourceController .....	406
A utilização desta política .....	406
Detalhes da política .....	406
Versão da política .....	406
Documento da política JSON .....	406
Saiba mais .....	407

AmazonEKSElasticContainerWorkerNodePolicy .....	407
Utilização desta política .....	407
Detalhes desta política .....	407
Versão da política .....	408
Documento da política JSON .....	408
Saiba mais .....	409
AmazonElasticCacheFullAccess .....	409
Utilização desta política .....	409
Detalhes desta política .....	409
Versão da política .....	409
Documento da política JSON .....	409
Saiba mais .....	413
AmazonElasticCacheReadOnlyAccess .....	413
A utilização desta política .....	413
Detalhes da política .....	413
Versão da política .....	413
Documento da política JSON .....	414
Saiba mais .....	414
AmazonElasticContainerRegistryPublicFullAccess .....	414
A utilização desta política .....	414
Detalhes da política .....	414
Versão da política .....	415
Documento da política JSON .....	415
Saiba mais .....	415
AmazonElasticContainerRegistryPublicPowerUser .....	416
A utilização desta política .....	416
Detalhes da política .....	416
Versão da política .....	416
Documento da política JSON .....	416
Saiba mais .....	417
AmazonElasticContainerRegistryPublicReadOnly .....	417
A utilização desta política .....	417
Detalhes da política .....	417
Versão da política .....	418
Documento da política JSON .....	418
Saiba mais .....	418

AmazonElasticFileSystemClientFullAccess .....	419
A utilização desta política .....	419
Detalhes da política .....	419
Versão da política .....	419
Documento da política JSON .....	419
Saiba mais .....	420
AmazonElasticFileSystemClientReadOnlyAccess .....	420
A utilização desta política .....	420
Detalhes da política .....	420
Versão da política .....	420
Documento da política JSON .....	421
Saiba mais .....	421
AmazonElasticFileSystemClientReadWriteAccess .....	421
A utilização desta política .....	421
Detalhes da política .....	422
Versão da política .....	422
Documento da política JSON .....	422
Saiba mais .....	422
AmazonElasticFileSystemFullAccess .....	423
Utilização desta política .....	423
Detalhes desta política .....	423
Versão da política .....	423
Documento da política JSON .....	423
Saiba mais .....	425
AmazonElasticFileSystemReadOnlyAccess .....	425
A utilização desta política .....	425
Detalhes da política .....	426
Versão da política .....	426
Documento da política JSON .....	426
Saiba mais .....	427
AmazonElasticFileSystemServiceRolePolicy .....	427
A utilização desta política .....	427
Detalhes da política .....	427
Versão da política .....	428
Documento da política JSON .....	428
Saiba mais .....	430

AmazonElasticFileSystemsUtils .....	430
A utilização desta política .....	430
Detalhes da política .....	430
Versão da política .....	430
Documento da política JSON .....	431
Saiba mais .....	432
AmazonElasticMapReduceEditorsRole .....	433
A utilização desta política .....	433
Detalhes da política .....	433
Versão da política .....	433
Documento da política JSON .....	433
Saiba mais .....	434
AmazonElasticMapReduceforAutoScalingRole .....	435
A utilização desta política .....	435
Detalhes da política .....	435
Versão da política .....	435
Documento da política JSON .....	435
Saiba mais .....	436
AmazonElasticMapReduceforEC2Role .....	436
A utilização desta política .....	436
Detalhes da política .....	436
Versão da política .....	437
Documento da política JSON .....	437
Saiba mais .....	438
AmazonElasticMapReduceFullAccess .....	438
A utilização desta política .....	439
Detalhes da política .....	439
Versão da política .....	439
Documento da política JSON .....	439
Saiba mais .....	441
AmazonElasticMapReducePlacementGroupPolicy .....	441
A utilização desta política .....	441
Detalhes da política .....	441
Versão da política .....	441
Documento da política JSON .....	442
Saiba mais .....	442

AmazonElasticMapReduceReadOnlyAccess .....	442
A utilização desta política .....	443
Detalhes da política .....	443
Versão da política .....	443
Documento da política JSON .....	443
Saiba mais .....	444
AmazonElasticMapReduceRole .....	444
A utilização desta política .....	444
Detalhes da política .....	444
Versão da política .....	444
Documento da política JSON .....	445
Saiba mais .....	447
AmazonElasticsearchServiceRolePolicy .....	447
A utilização desta política .....	447
Detalhes da política .....	447
Versão da política .....	447
Documento da política JSON .....	448
Saiba mais .....	450
AmazonElasticTranscoder_FullAccess .....	451
A utilização desta política .....	451
Detalhes da política .....	451
Versão da política .....	451
Documento da política JSON .....	451
Saiba mais .....	452
AmazonElasticTranscoder_JobsSubmitter .....	452
A utilização desta política .....	452
Detalhes da política .....	453
Versão da política .....	453
Documento da política JSON .....	453
Saiba mais .....	453
AmazonElasticTranscoder_ReadOnlyAccess .....	454
A utilização desta política .....	454
Detalhes da política .....	454
Versão da política .....	454
Documento da política JSON .....	454
Saiba mais .....	455

AmazonElasticTranscoderRole .....	455
A utilização desta política .....	455
Detalhes da política .....	455
Versão da política .....	456
Documento da política JSON .....	456
Saiba mais .....	457
AmazonEMRCleanupPolicy .....	457
A utilização desta política .....	457
Detalhes da política .....	457
Versão da política .....	457
Documento da política JSON .....	457
Saiba mais .....	458
AmazonEMRContainersServiceRolePolicy .....	458
A utilização desta política .....	458
Detalhes da política .....	459
Versão da política .....	459
Documento da política JSON .....	459
Saiba mais .....	460
AmazonEMRFullAccessPolicy_v2 .....	460
A utilização desta política .....	460
Detalhes da política .....	461
Versão da política .....	461
Documento da política JSON .....	461
Saiba mais .....	464
AmazonEMRReadOnlyAccessPolicy_v2 .....	465
A utilização desta política .....	465
Detalhes da política .....	465
Versão da política .....	465
Documento da política JSON .....	465
Saiba mais .....	466
AmazonEMRServerlessServiceRolePolicy .....	466
Utilização desta política .....	467
Detalhes desta política .....	467
Versão da política .....	467
Documento da política JSON .....	467
Saiba mais .....	468

AmazonEMRServicePolicy_v2 .....	468
A utilização desta política .....	468
Detalhes da política .....	469
Versão da política .....	469
Documento da política JSON .....	469
Saiba mais .....	476
AmazonESCognitoAccess .....	477
A utilização desta política .....	477
Detalhes da política .....	477
Versão da política .....	477
Documento da política JSON .....	477
Saiba mais .....	478
AmazonESFullAccess .....	479
A utilização desta política .....	479
Detalhes da política .....	479
Versão da política .....	479
Documento da política JSON .....	479
Saiba mais .....	480
AmazonESReadOnlyAccess .....	480
A utilização desta política .....	480
Detalhes da política .....	480
Versão da política .....	480
Documento da política JSON .....	480
Saiba mais .....	481
AmazonEventBridgeApiDestinationsServiceRolePolicy .....	481
A utilização desta política .....	481
Detalhes da política .....	481
Versão da política .....	482
Documento da política JSON .....	482
Saiba mais .....	482
AmazonEventBridgeFullAccess .....	482
A utilização desta política .....	483
Detalhes da política .....	483
Versão da política .....	483
Documento da política JSON .....	483
Saiba mais .....	485

AmazonEventBridgePipesFullAccess .....	485
A utilização desta política .....	485
Detalhes da política .....	486
Versão da política .....	486
Documento da política JSON .....	486
Saiba mais .....	487
AmazonEventBridgePipesOperatorAccess .....	487
A utilização desta política .....	487
Detalhes da política .....	487
Versão da política .....	487
Documento da política JSON .....	487
Saiba mais .....	488
AmazonEventBridgePipesReadOnlyAccess .....	488
A utilização desta política .....	488
Detalhes da política .....	488
Versão da política .....	489
Documento da política JSON .....	489
Saiba mais .....	489
AmazonEventBridgeReadOnlyAccess .....	490
A utilização desta política .....	490
Detalhes da política .....	490
Versão da política .....	490
Documento da política JSON .....	490
Saiba mais .....	491
AmazonEventBridgeSchedulerFullAccess .....	492
A utilização desta política .....	492
Detalhes da política .....	492
Versão da política .....	492
Documento da política JSON .....	492
Saiba mais .....	493
AmazonEventBridgeSchedulerReadOnlyAccess .....	493
A utilização desta política .....	493
Detalhes da política .....	493
Versão da política .....	494
Documento da política JSON .....	494
Saiba mais .....	494



AmazonEventBridgeSchemasFullAccess .....	495
A utilização desta política .....	495
Detalhes da política .....	495
Versão da política .....	495
Documento da política JSON .....	495
Saiba mais .....	496
AmazonEventBridgeSchemasReadOnlyAccess .....	496
A utilização desta política .....	496
Detalhes da política .....	497
Versão da política .....	497
Documento da política JSON .....	497
Saiba mais .....	498
AmazonEventBridgeSchemasServiceRolePolicy .....	498
A utilização desta política .....	498
Detalhes da política .....	498
Versão da política .....	498
Documento da política JSON .....	499
Saiba mais .....	499
AmazonFISServiceRolePolicy .....	499
A utilização desta política .....	499
Detalhes da política .....	500
Versão da política .....	500
Documento da política JSON .....	500
Saiba mais .....	502
AmazonForecastFullAccess .....	502
A utilização desta política .....	502
Detalhes da política .....	502
Versão da política .....	502
Documento da política JSON .....	502
Saiba mais .....	503
AmazonFraudDetectorFullAccessPolicy .....	503
A utilização desta política .....	503
Detalhes da política .....	503
Versão da política .....	504
Documento da política JSON .....	504
Saiba mais .....	505

AmazonFreeRTOSFullAccess .....	505
A utilização desta política .....	505
Detalhes da política .....	506
Versão da política .....	506
Documento da política JSON .....	506
Saiba mais .....	506
AmazonFreeRTOSOTAUpdate .....	507
A utilização desta política .....	507
Detalhes da política .....	507
Versão da política .....	507
Documento da política JSON .....	507
Saiba mais .....	509
AmazonFSxConsoleFullAccess .....	509
Utilização desta política .....	509
Detalhes desta política .....	509
Versão da política .....	509
Documento da política JSON .....	509
Saiba mais .....	513
AmazonFSxConsoleReadOnlyAccess .....	513
Utilização desta política .....	513
Detalhes desta política .....	513
Versão da política .....	514
Documento da política JSON .....	514
Saiba mais .....	514
AmazonFSxFullAccess .....	515
Utilização desta política .....	515
Detalhes desta política .....	515
Versão da política .....	515
Documento da política JSON .....	515
Saiba mais .....	519
AmazonFSxReadOnlyAccess .....	520
A utilização desta política .....	520
Detalhes da política .....	520
Versão da política .....	520
Documento da política JSON .....	520
Saiba mais .....	521

AmazonFSxServiceRolePolicy .....	521
Utilização desta política .....	521
Detalhes desta política .....	521
Versão da política .....	521
Documento da política JSON .....	522
Saiba mais .....	524
AmazonGlacierFullAccess .....	524
A utilização desta política .....	525
Detalhes da política .....	525
Versão da política .....	525
Documento da política JSON .....	525
Saiba mais .....	525
AmazonGlacierReadOnlyAccess .....	526
A utilização desta política .....	526
Detalhes da política .....	526
Versão da política .....	526
Documento da política JSON .....	526
Saiba mais .....	527
AmazonGrafanaAthenaAccess .....	527
A utilização desta política .....	527
Detalhes da política .....	527
Versão da política .....	528
Documento da política JSON .....	528
Saiba mais .....	529
AmazonGrafanaCloudWatchAccess .....	530
A utilização desta política .....	530
Detalhes da política .....	530
Versão da política .....	530
Documento da política JSON .....	530
Saiba mais .....	532
AmazonGrafanaRedshiftAccess .....	532
A utilização desta política .....	532
Detalhes da política .....	532
Versão da política .....	532
Documento da política JSON .....	533
Saiba mais .....	534

AmazonGrafanaServiceLinkedRolePolicy .....	534
A utilização desta política .....	534
Detalhes da política .....	534
Versão da política .....	535
Documento da política JSON .....	535
Saiba mais .....	536
AmazonGuardDutyFullAccess .....	536
Utilização desta política .....	536
Detalhes desta política .....	536
Versão da política .....	537
Documento da política JSON .....	537
Saiba mais .....	538
AmazonGuardDutyMalwareProtectionServiceRolePolicy .....	538
Utilização desta política .....	539
Detalhes desta política .....	539
Versão da política .....	539
Documento da política JSON .....	539
Saiba mais .....	544
AmazonGuardDutyReadOnlyAccess .....	544
Utilização desta política .....	544
Detalhes desta política .....	544
Versão da política .....	544
Documento da política JSON .....	544
Saiba mais .....	545
AmazonGuardDutyServiceRolePolicy .....	545
Utilização desta política .....	546
Detalhes desta política .....	546
Versão da política .....	546
Documento da política JSON .....	546
Saiba mais .....	551
AmazonHealthLakeFullAccess .....	551
A utilização desta política .....	551
Detalhes da política .....	551
Versão da política .....	551
Documento da política JSON .....	552
Saiba mais .....	552

AmazonHealthLakeReadOnlyAccess .....	553
A utilização desta política .....	553
Detalhes da política .....	553
Versão da política .....	553
Documento da política JSON .....	553
Saiba mais .....	554
AmazonHoneycodeFullAccess .....	554
A utilização desta política .....	554
Detalhes da política .....	554
Versão da política .....	554
Documento da política JSON .....	555
Saiba mais .....	555
AmazonHoneycodeReadOnlyAccess .....	555
A utilização desta política .....	555
Detalhes da política .....	555
Versão da política .....	556
Documento da política JSON .....	556
Saiba mais .....	556
AmazonHoneycodeServiceRolePolicy .....	556
A utilização desta política .....	557
Detalhes da política .....	557
Versão da política .....	557
Documento da política JSON .....	557
Saiba mais .....	557
AmazonHoneycodeTeamAssociationFullAccess .....	558
A utilização desta política .....	558
Detalhes da política .....	558
Versão da política .....	558
Documento da política JSON .....	558
Saiba mais .....	559
AmazonHoneycodeTeamAssociationReadOnlyAccess .....	559
A utilização desta política .....	559
Detalhes da política .....	559
Versão da política .....	559
Documento da política JSON .....	560
Saiba mais .....	560

AmazonHoneycodeWorkbookFullAccess .....	560
A utilização desta política .....	560
Detalhes da política .....	561
Versão da política .....	561
Documento da política JSON .....	561
Saiba mais .....	562
AmazonHoneycodeWorkbookReadOnlyAccess .....	562
A utilização desta política .....	562
Detalhes da política .....	562
Versão da política .....	562
Documento da política JSON .....	562
Saiba mais .....	563
AmazonInspector2AgentlessServiceRolePolicy .....	563
A utilização desta política .....	563
Detalhes desta política .....	563
Versão da política .....	564
Documento da política JSON .....	564
Saiba mais .....	567
AmazonInspector2FullAccess .....	568
A utilização desta política .....	568
Detalhes da política .....	568
Versão da política .....	568
Documento da política JSON .....	568
Saiba mais .....	569
AmazonInspector2ManagedCisPolicy .....	570
Utilização desta política .....	570
Detalhes desta política .....	570
Versão da política .....	570
Documento da política JSON .....	570
Saiba mais .....	571
AmazonInspector2ReadOnlyAccess .....	571
A utilização desta política .....	571
Detalhes da política .....	571
Versão da política .....	571
Documento da política JSON .....	572
Saiba mais .....	572

AmazonInspector2ServiceRolePolicy .....	572
Utilização desta política .....	573
Detalhes desta política .....	573
Versão da política .....	573
Documento da política JSON .....	573
Saiba mais .....	579
AmazonInspectorFullAccess .....	580
A utilização desta política .....	580
Detalhes da política .....	580
Versão da política .....	580
Documento da política JSON .....	580
Saiba mais .....	581
AmazonInspectorReadOnlyAccess .....	582
A utilização desta política .....	582
Detalhes da política .....	582
Versão da política .....	582
Documento da política JSON .....	582
Saiba mais .....	583
AmazonInspectorServiceRolePolicy .....	583
A utilização desta política .....	583
Detalhes da política .....	583
Versão da política .....	583
Documento da política JSON .....	584
Saiba mais .....	585
AmazonKendraFullAccess .....	585
A utilização desta política .....	585
Detalhes da política .....	585
Versão da política .....	586
Documento da política JSON .....	586
Saiba mais .....	588
AmazonKendraReadOnlyAccess .....	588
A utilização desta política .....	588
Detalhes da política .....	588
Versão da política .....	588
Documento da política JSON .....	588
Saiba mais .....	589

AmazonKeyspacesFullAccess .....	589
A utilização desta política .....	589
Detalhes da política .....	589
Versão da política .....	590
Documento da política JSON .....	590
Saiba mais .....	592
AmazonKeyspacesReadOnlyAccess .....	592
A utilização desta política .....	592
Detalhes da política .....	592
Versão da política .....	592
Documento da política JSON .....	592
Saiba mais .....	593
AmazonKeyspacesReadOnlyAccess_v2 .....	593
A utilização desta política .....	593
Detalhes da política .....	594
Versão da política .....	594
Documento da política JSON .....	594
Saiba mais .....	595
AmazonKinesisAnalyticsFullAccess .....	595
A utilização desta política .....	595
Detalhes da política .....	595
Versão da política .....	596
Documento da política JSON .....	596
Saiba mais .....	597
AmazonKinesisAnalyticsReadOnly .....	597
A utilização desta política .....	597
Detalhes da política .....	598
Versão da política .....	598
Documento da política JSON .....	598
Saiba mais .....	599
AmazonKinesisFirehoseFullAccess .....	600
A utilização desta política .....	600
Detalhes da política .....	600
Versão da política .....	600
Documento da política JSON .....	600
Saiba mais .....	601



AmazonKinesisFirehoseReadOnlyAccess .....	601
A utilização desta política .....	601
Detalhes da política .....	601
Versão da política .....	601
Documento da política JSON .....	601
Saiba mais .....	602
AmazonKinesisFullAccess .....	602
A utilização desta política .....	602
Detalhes da política .....	602
Versão da política .....	603
Documento da política JSON .....	603
Saiba mais .....	603
AmazonKinesisReadOnlyAccess .....	603
A utilização desta política .....	603
Detalhes da política .....	604
Versão da política .....	604
Documento da política JSON .....	604
Saiba mais .....	604
AmazonKinesisVideoStreamsFullAccess .....	605
A utilização desta política .....	605
Detalhes da política .....	605
Versão da política .....	605
Documento da política JSON .....	605
Saiba mais .....	606
AmazonKinesisVideoStreamsReadOnlyAccess .....	606
A utilização desta política .....	606
Detalhes da política .....	606
Versão da política .....	606
Documento da política JSON .....	607
Saiba mais .....	607
AmazonLaunchWizard_Fullaccess .....	607
A utilização desta política .....	607
Detalhes da política .....	607
Versão da política .....	608
Documento da política JSON .....	608
Saiba mais .....	622

AmazonLaunchWizardFullAccessV2 .....	622
A utilização desta política .....	622
Detalhes da política .....	622
Versão da política .....	623
Documento da política JSON .....	623
Saiba mais .....	639
AmazonLexChannelsAccess .....	640
A utilização desta política .....	640
Detalhes da política .....	640
Versão da política .....	640
Documento da política JSON .....	640
Saiba mais .....	641
AmazonLexFullAccess .....	641
Utilização desta política .....	641
Detalhes desta política .....	641
Versão da política .....	641
Documento da política JSON .....	641
Saiba mais .....	647
AmazonLexReadOnly .....	647
A utilização desta política .....	647
Detalhes da política .....	647
Versão da política .....	647
Documento da política JSON .....	648
Saiba mais .....	649
AmazonLexReplicationPolicy .....	649
Utilização desta política .....	649
Detalhes desta política .....	650
Versão da política .....	650
Documento da política JSON .....	650
Saiba mais .....	652
AmazonLexRunBotsOnly .....	652
A utilização desta política .....	652
Detalhes da política .....	652
Versão da política .....	653
Documento da política JSON .....	653
Saiba mais .....	653

AmazonLexV2BotPolicy .....	654
A utilização desta política .....	654
Detalhes da política .....	654
Versão da política .....	654
Documento da política JSON .....	654
Saiba mais .....	655
AmazonLookoutEquipmentFullAccess .....	655
A utilização desta política .....	655
Detalhes da política .....	655
Versão da política .....	655
Documento da política JSON .....	656
Saiba mais .....	657
AmazonLookoutEquipmentReadOnlyAccess .....	657
A utilização desta política .....	657
Detalhes da política .....	657
Versão da política .....	657
Documento da política JSON .....	658
Saiba mais .....	658
AmazonLookoutMetricsFullAccess .....	658
A utilização desta política .....	658
Detalhes da política .....	659
Versão da política .....	659
Documento da política JSON .....	659
Saiba mais .....	660
AmazonLookoutMetricsReadOnlyAccess .....	660
A utilização desta política .....	660
Detalhes da política .....	660
Versão da política .....	660
Documento da política JSON .....	661
Saiba mais .....	661
AmazonLookoutVisionConsoleFullAccess .....	662
A utilização desta política .....	662
Detalhes da política .....	662
Versão da política .....	662
Documento da política JSON .....	662
Saiba mais .....	664

AmazonLookoutVisionConsoleReadOnlyAccess .....	665
A utilização desta política .....	665
Detalhes da política .....	665
Versão da política .....	665
Documento da política JSON .....	665
Saiba mais .....	667
AmazonLookoutVisionFullAccess .....	667
A utilização desta política .....	667
Detalhes da política .....	667
Versão da política .....	667
Documento da política JSON .....	667
Saiba mais .....	668
AmazonLookoutVisionReadOnlyAccess .....	668
A utilização desta política .....	668
Detalhes da política .....	668
Versão da política .....	669
Documento da política JSON .....	669
Saiba mais .....	669
AmazonMachineLearningBatchPredictionsAccess .....	670
A utilização desta política .....	670
Detalhes da política .....	670
Versão da política .....	670
Documento da política JSON .....	670
Saiba mais .....	671
AmazonMachineLearningCreateOnlyAccess .....	671
A utilização desta política .....	671
Detalhes da política .....	671
Versão da política .....	671
Documento da política JSON .....	672
Saiba mais .....	672
AmazonMachineLearningFullAccess .....	672
A utilização desta política .....	672
Detalhes da política .....	672
Versão da política .....	673
Documento da política JSON .....	673
Saiba mais .....	673

AmazonMachineLearningManageRealTimeEndpointOnlyAccess .....	674
A utilização desta política .....	674
Detalhes da política .....	674
Versão da política .....	674
Documento da política JSON .....	674
Saiba mais .....	675
AmazonMachineLearningReadOnlyAccess .....	675
A utilização desta política .....	675
Detalhes da política .....	675
Versão da política .....	675
Documento da política JSON .....	676
Saiba mais .....	676
AmazonMachineLearningRealTimePredictionOnlyAccess .....	676
A utilização desta política .....	676
Detalhes da política .....	676
Versão da política .....	677
Documento da política JSON .....	677
Saiba mais .....	677
AmazonMachineLearningRoleforRedshiftDataSourceV3 .....	678
A utilização desta política .....	678
Detalhes da política .....	678
Versão da política .....	678
Documento da política JSON .....	678
Saiba mais .....	679
AmazonMacieFullAccess .....	679
A utilização desta política .....	679
Detalhes da política .....	680
Versão da política .....	680
Documento da política JSON .....	680
Saiba mais .....	681
AmazonMacieHandshakeRole .....	681
A utilização desta política .....	681
Detalhes da política .....	681
Versão da política .....	681
Documento da política JSON .....	682
Saiba mais .....	682

AmazonMacieReadOnlyAccess .....	682
A utilização desta política .....	682
Detalhes da política .....	682
Versão da política .....	683
Documento da política JSON .....	683
Saiba mais .....	683
AmazonMacieServiceRole .....	684
A utilização desta política .....	684
Detalhes da política .....	684
Versão da política .....	684
Documento da política JSON .....	684
Saiba mais .....	685
AmazonMacieServiceRolePolicy .....	685
A utilização desta política .....	685
Detalhes da política .....	685
Versão da política .....	685
Documento da política JSON .....	686
Saiba mais .....	687
AmazonManagedBlockchainConsoleFullAccess .....	687
A utilização desta política .....	687
Detalhes da política .....	687
Versão da política .....	687
Documento da política JSON .....	688
Saiba mais .....	688
AmazonManagedBlockchainFullAccess .....	688
A utilização desta política .....	689
Detalhes da política .....	689
Versão da política .....	689
Documento da política JSON .....	689
Saiba mais .....	690
AmazonManagedBlockchainReadOnlyAccess .....	690
A utilização desta política .....	690
Detalhes da política .....	690
Versão da política .....	690
Documento da política JSON .....	690
Saiba mais .....	691

AmazonManagedBlockchainServiceRolePolicy .....	691
A utilização desta política .....	691
Detalhes da política .....	691
Versão da política .....	692
Documento da política JSON .....	692
Saiba mais .....	692
AmazonMCSFullAccess .....	693
A utilização desta política .....	693
Detalhes da política .....	693
Versão da política .....	693
Documento da política JSON .....	693
Saiba mais .....	694
AmazonMCSReadOnlyAccess .....	695
A utilização desta política .....	695
Detalhes da política .....	695
Versão da política .....	695
Documento da política JSON .....	695
Saiba mais .....	696
AmazonMechanicalTurkFullAccess .....	696
A utilização desta política .....	696
Detalhes da política .....	696
Versão da política .....	697
Documento da política JSON .....	697
Saiba mais .....	697
AmazonMechanicalTurkReadOnly .....	698
A utilização desta política .....	698
Detalhes da política .....	698
Versão da política .....	698
Documento da política JSON .....	698
Saiba mais .....	699
AmazonMemoryDBFullAccess .....	699
A utilização desta política .....	699
Detalhes da política .....	699
Versão da política .....	699
Documento da política JSON .....	699
Saiba mais .....	700

AmazonMemoryDBReadOnlyAccess .....	700
A utilização desta política .....	700
Detalhes da política .....	701
Versão da política .....	701
Documento da política JSON .....	701
Saiba mais .....	701
AmazonMobileAnalyticsFinancialReportAccess .....	702
A utilização desta política .....	702
Detalhes da política .....	702
Versão da política .....	702
Documento da política JSON .....	702
Saiba mais .....	703
AmazonMobileAnalyticsFullAccess .....	703
A utilização desta política .....	703
Detalhes da política .....	703
Versão da política .....	703
Documento da política JSON .....	704
Saiba mais .....	704
AmazonMobileAnalyticsNon-financialReportAccess .....	704
A utilização desta política .....	704
Detalhes da política .....	704
Versão da política .....	705
Documento da política JSON .....	705
Saiba mais .....	705
AmazonMobileAnalyticsWriteOnlyAccess .....	705
A utilização desta política .....	706
Detalhes da política .....	706
Versão da política .....	706
Documento da política JSON .....	706
Saiba mais .....	706
AmazonMonitronFullAccess .....	707
A utilização desta política .....	707
Detalhes da política .....	707
Versão da política .....	707
Documento da política JSON .....	707
Saiba mais .....	709



AmazonMQApiFullAccess .....	709
A utilização desta política .....	709
Detalhes da política .....	710
Versão da política .....	710
Documento da política JSON .....	710
Saiba mais .....	711
AmazonMQApiReadOnlyAccess .....	711
A utilização desta política .....	711
Detalhes da política .....	712
Versão da política .....	712
Documento da política JSON .....	712
Saiba mais .....	712
AmazonMQFullAccess .....	713
A utilização desta política .....	713
Detalhes da política .....	713
Versão da política .....	713
Documento da política JSON .....	713
Saiba mais .....	714
AmazonMQReadOnlyAccess .....	715
A utilização desta política .....	715
Detalhes da política .....	715
Versão da política .....	715
Documento da política JSON .....	715
Saiba mais .....	716
AmazonMQServiceRolePolicy .....	716
A utilização desta política .....	716
Detalhes da política .....	716
Versão da política .....	717
Documento da política JSON .....	717
Saiba mais .....	719
AmazonMSKConnectReadOnlyAccess .....	719
A utilização desta política .....	719
Detalhes da política .....	719
Versão da política .....	719
Documento da política JSON .....	719
Saiba mais .....	720

---

AmazonMSKFullAccess .....	721
A utilização desta política .....	721
Detalhes da política .....	721
Versão da política .....	721
Documento da política JSON .....	721
Saiba mais .....	724
AmazonMSKReadOnlyAccess .....	724
A utilização desta política .....	724
Detalhes da política .....	724
Versão da política .....	725
Documento da política JSON .....	725
Saiba mais .....	725
AmazonMWAAServiceRolePolicy .....	726
A utilização desta política .....	726
Detalhes da política .....	726
Versão da política .....	726
Documento da política JSON .....	726
Saiba mais .....	728
AmazonNimbleStudio-LaunchProfileWorker .....	729
A utilização desta política .....	729
Detalhes da política .....	729
Versão da política .....	729
Documento da política JSON .....	729
Saiba mais .....	730
AmazonNimbleStudio-StudioAdmin .....	730
A utilização desta política .....	730
Detalhes da política .....	730
Versão da política .....	731
Documento da política JSON .....	731
Saiba mais .....	733
AmazonNimbleStudio-StudioUser .....	733
A utilização desta política .....	733
Detalhes da política .....	733
Versão da política .....	733
Documento da política JSON .....	734
Saiba mais .....	736

---

AmazonOmicsFullAccess .....	736
A utilização desta política .....	736
Detalhes da política .....	736
Versão da política .....	736
Documento da política JSON .....	737
Saiba mais .....	737
AmazonOmicsReadOnlyAccess .....	738
A utilização desta política .....	738
Detalhes da política .....	738
Versão da política .....	738
Documento da política JSON .....	738
Saiba mais .....	739
AmazonOneEnterpriseFullAccess .....	739
Utilização desta política .....	739
Detalhes desta política .....	739
Versão da política .....	739
Documento da política JSON .....	740
Saiba mais .....	740
AmazonOneEnterpriseInstallerAccess .....	740
Utilização desta política .....	741
Detalhes desta política .....	741
Versão da política .....	741
Documento da política JSON .....	741
Saiba mais .....	742
AmazonOneEnterpriseReadOnlyAccess .....	742
Utilização desta política .....	742
Detalhes desta política .....	742
Versão da política .....	742
Documento da política JSON .....	743
Saiba mais .....	743
AmazonOpenSearchDashboardsServiceRolePolicy .....	743
A utilização desta política .....	743
Detalhes desta política .....	744
Versão da política .....	744
Documento da política JSON .....	744
Saiba mais .....	744

AmazonOpenSearchIngestionFullAccess .....	745
A utilização desta política .....	745
Detalhes da política .....	745
Versão da política .....	745
Documento da política JSON .....	745
Saiba mais .....	746
AmazonOpenSearchIngestionReadOnlyAccess .....	746
A utilização desta política .....	747
Detalhes da política .....	747
Versão da política .....	747
Documento da política JSON .....	747
Saiba mais .....	748
AmazonOpenSearchIngestionServiceRolePolicy .....	748
A utilização desta política .....	748
Detalhes da política .....	748
Versão da política .....	748
Documento da política JSON .....	748
Saiba mais .....	750
AmazonOpenSearchServerlessServiceRolePolicy .....	750
A utilização desta política .....	751
Detalhes da política .....	751
Versão da política .....	751
Documento da política JSON .....	751
Saiba mais .....	752
AmazonOpenSearchServiceCognitoAccess .....	752
A utilização desta política .....	752
Detalhes da política .....	752
Versão da política .....	752
Documento da política JSON .....	752
Saiba mais .....	753
AmazonOpenSearchServiceFullAccess .....	754
A utilização desta política .....	754
Detalhes da política .....	754
Versão da política .....	754
Documento da política JSON .....	754
Saiba mais .....	755

---

AmazonOpenSearchServiceReadOnlyAccess .....	755
A utilização desta política .....	755
Detalhes da política .....	755
Versão da política .....	755
Documento da política JSON .....	756
Saiba mais .....	756
AmazonOpenSearchServiceRolePolicy .....	756
A utilização desta política .....	756
Detalhes da política .....	757
Versão da política .....	757
Documento da política JSON .....	757
Saiba mais .....	762
AmazonPersonalizeFullAccess .....	762
A utilização desta política .....	762
Detalhes da política .....	762
Versão da política .....	762
Documento da política JSON .....	762
Saiba mais .....	764
AmazonPollyFullAccess .....	764
A utilização desta política .....	764
Detalhes da política .....	764
Versão da política .....	764
Documento da política JSON .....	764
Saiba mais .....	765
AmazonPollyReadOnlyAccess .....	765
A utilização desta política .....	765
Detalhes da política .....	765
Versão da política .....	766
Documento da política JSON .....	766
Saiba mais .....	766
AmazonPrometheusConsoleFullAccess .....	767
A utilização desta política .....	767
Detalhes da política .....	767
Versão da política .....	767
Documento da política JSON .....	767
Saiba mais .....	768

AmazonPrometheusFullAccess .....	768
Utilização desta política .....	769
Detalhes desta política .....	769
Versão da política .....	769
Documento da política JSON .....	769
Saiba mais .....	770
AmazonPrometheusQueryAccess .....	770
A utilização desta política .....	771
Detalhes da política .....	771
Versão da política .....	771
Documento da política JSON .....	771
Saiba mais .....	772
AmazonPrometheusRemoteWriteAccess .....	772
A utilização desta política .....	772
Detalhes da política .....	772
Versão da política .....	772
Documento da política JSON .....	772
Saiba mais .....	773
AmazonPrometheusScrapperServiceRolePolicy .....	773
A utilização desta política .....	773
Detalhes desta política .....	773
Versão da política .....	774
Documento da política JSON .....	774
Saiba mais .....	776
AmazonQFullAccess .....	776
Utilização desta política .....	776
Detalhes desta política .....	776
Versão da política .....	776
Documento da política JSON .....	777
Saiba mais .....	777
AmazonQLDBConsoleFullAccess .....	777
A utilização desta política .....	777
Detalhes da política .....	777
Versão da política .....	778
Documento da política JSON .....	778
Saiba mais .....	780

AmazonQLDBFullAccess .....	780
A utilização desta política .....	780
Detalhes da política .....	780
Versão da política .....	780
Documento da política JSON .....	780
Saiba mais .....	782
AmazonQLDBReadOnly .....	782
A utilização desta política .....	782
Detalhes da política .....	782
Versão da política .....	782
Documento da política JSON .....	783
Saiba mais .....	783
AmazonRDSBetaServiceRolePolicy .....	784
A utilização desta política .....	784
Detalhes da política .....	784
Versão da política .....	784
Documento da política JSON .....	784
Saiba mais .....	787
AmazonRDSCustomInstanceProfileRolePolicy .....	788
Utilização desta política .....	788
Detalhes desta política .....	788
Versão da política .....	788
Documento da política JSON .....	788
Saiba mais .....	795
AmazonRDSCustomPreviewServiceRolePolicy .....	796
A utilização desta política .....	796
Detalhes da política .....	796
Versão da política .....	796
Documento da política JSON .....	796
Saiba mais .....	812
AmazonRDSCustomServiceRolePolicy .....	812
A utilização desta política .....	812
Detalhes da política .....	812
Versão da política .....	812
Documento da política JSON .....	813
Saiba mais .....	829

AmazonRDSDataFullAccess .....	830
A utilização desta política .....	830
Detalhes da política .....	830
Versão da política .....	830
Documento da política JSON .....	830
Saiba mais .....	831
AmazonRDSDirectoryServiceAccess .....	832
A utilização desta política .....	832
Detalhes da política .....	832
Versão da política .....	832
Documento da política JSON .....	832
Saiba mais .....	833
AmazonRDSEnhancedMonitoringRole .....	833
A utilização desta política .....	833
Detalhes da política .....	833
Versão da política .....	833
Documento da política JSON .....	834
Saiba mais .....	834
AmazonRDSFullAccess .....	835
A utilização desta política .....	835
Detalhes da política .....	835
Versão da política .....	835
Documento da política JSON .....	835
Saiba mais .....	837
AmazonRDSPerformancelnsightsFullAccess .....	837
A utilização desta política .....	838
Detalhes da política .....	838
Versão da política .....	838
Documento da política JSON .....	838
Saiba mais .....	840
AmazonRDSPerformancelnsightsReadOnly .....	840
A utilização desta política .....	840
Detalhes da política .....	840
Versão da política .....	840
Documento da política JSON .....	840
Saiba mais .....	842



AmazonRDSPreviewServiceRolePolicy .....	842
A utilização desta política .....	843
Detalhes da política .....	843
Versão da política .....	843
Documento da política JSON .....	843
Saiba mais .....	846
AmazonRDSReadOnlyAccess .....	846
A utilização desta política .....	847
Detalhes da política .....	847
Versão da política .....	847
Documento da política JSON .....	847
Saiba mais .....	848
AmazonRDSServiceRolePolicy .....	849
Utilização desta política .....	849
Detalhes desta política .....	849
Versão da política .....	849
Documento da política JSON .....	849
Saiba mais .....	853
AmazonRedshiftAllCommandsFullAccess .....	853
A utilização desta política .....	854
Detalhes da política .....	854
Versão da política .....	854
Documento da política JSON .....	854
Saiba mais .....	859
AmazonRedshiftDataFullAccess .....	860
A utilização desta política .....	860
Detalhes da política .....	860
Versão da política .....	860
Documento da política JSON .....	860
Saiba mais .....	862
AmazonRedshiftFullAccess .....	862
A utilização desta política .....	863
Detalhes da política .....	863
Versão da política .....	863
Documento da política JSON .....	863
Saiba mais .....	865

AmazonRedshiftQueryEditor .....	865
A utilização desta política .....	865
Detalhes da política .....	866
Versão da política .....	866
Documento da política JSON .....	866
Saiba mais .....	868
AmazonRedshiftQueryEditorV2FullAccess .....	868
Utilização desta política .....	868
Detalhes desta política .....	868
Versão da política .....	869
Documento da política JSON .....	869
Saiba mais .....	870
AmazonRedshiftQueryEditorV2NoSharing .....	870
Utilização desta política .....	871
Detalhes desta política .....	871
Versão da política .....	871
Documento da política JSON .....	871
Saiba mais .....	875
AmazonRedshiftQueryEditorV2ReadSharing .....	875
Utilização desta política .....	875
Detalhes desta política .....	875
Versão da política .....	875
Documento da política JSON .....	876
Saiba mais .....	880
AmazonRedshiftQueryEditorV2ReadWriteSharing .....	881
Utilização desta política .....	881
Detalhes desta política .....	881
Versão da política .....	881
Documento da política JSON .....	881
Saiba mais .....	886
AmazonRedshiftReadOnlyAccess .....	887
Utilização desta política .....	887
Detalhes desta política .....	887
Versão da política .....	887
Documento da política JSON .....	887
Saiba mais .....	888

AmazonRedshiftServiceLinkedRolePolicy .....	888
Utilização desta política .....	888
Detalhes desta política .....	888
Versão da política .....	889
Documento da política JSON .....	889
Saiba mais .....	894
AmazonRekognitionCustomLabelsFullAccess .....	894
A utilização desta política .....	895
Detalhes da política .....	895
Versão da política .....	895
Documento da política JSON .....	895
Saiba mais .....	896
AmazonRekognitionFullAccess .....	897
A utilização desta política .....	897
Detalhes da política .....	897
Versão da política .....	897
Documento da política JSON .....	897
Saiba mais .....	898
AmazonRekognitionReadOnlyAccess .....	898
Utilização desta política .....	898
Detalhes desta política .....	898
Versão da política .....	898
Documento da política JSON .....	898
Saiba mais .....	900
AmazonRekognitionServiceRole .....	900
A utilização desta política .....	900
Detalhes da política .....	900
Versão da política .....	900
Documento da política JSON .....	901
Saiba mais .....	901
AmazonRoute53AutoNamingFullAccess .....	902
A utilização desta política .....	902
Detalhes da política .....	902
Versão da política .....	902
Documento da política JSON .....	902
Saiba mais .....	903

AmazonRoute53AutoNamingReadOnlyAccess .....	903
A utilização desta política .....	903
Detalhes da política .....	903
Versão da política .....	904
Documento da política JSON .....	904
Saiba mais .....	904
AmazonRoute53AutoNamingRegistrantAccess .....	904
A utilização desta política .....	905
Detalhes da política .....	905
Versão da política .....	905
Documento da política JSON .....	905
Saiba mais .....	906
AmazonRoute53DomainsFullAccess .....	906
A utilização desta política .....	906
Detalhes da política .....	906
Versão da política .....	906
Documento da política JSON .....	907
Saiba mais .....	907
AmazonRoute53DomainsReadOnlyAccess .....	907
A utilização desta política .....	907
Detalhes da política .....	908
Versão da política .....	908
Documento da política JSON .....	908
Saiba mais .....	908
AmazonRoute53FullAccess .....	909
A utilização desta política .....	909
Detalhes da política .....	909
Versão da política .....	909
Documento da política JSON .....	909
Saiba mais .....	910
AmazonRoute53ReadOnlyAccess .....	910
A utilização desta política .....	910
Detalhes da política .....	911
Versão da política .....	911
Documento da política JSON .....	911
Saiba mais .....	911

AmazonRoute53RecoveryClusterFullAccess .....	912
A utilização desta política .....	912
Detalhes da política .....	912
Versão da política .....	912
Documento da política JSON .....	912
Saiba mais .....	913
AmazonRoute53RecoveryClusterReadOnlyAccess .....	913
A utilização desta política .....	913
Detalhes da política .....	913
Versão da política .....	913
Documento da política JSON .....	914
Saiba mais .....	914
AmazonRoute53RecoveryControlConfigFullAccess .....	914
A utilização desta política .....	914
Detalhes da política .....	914
Versão da política .....	915
Documento da política JSON .....	915
Saiba mais .....	915
AmazonRoute53RecoveryControlConfigReadOnlyAccess .....	915
A utilização desta política .....	916
Detalhes da política .....	916
Versão da política .....	916
Documento da política JSON .....	916
Saiba mais .....	917
AmazonRoute53RecoveryReadinessFullAccess .....	917
A utilização desta política .....	917
Detalhes da política .....	917
Versão da política .....	917
Documento da política JSON .....	918
Saiba mais .....	918
AmazonRoute53RecoveryReadinessReadOnlyAccess .....	918
A utilização desta política .....	918
Detalhes da política .....	919
Versão da política .....	919
Documento da política JSON .....	919
Saiba mais .....	920

AmazonRoute53ResolverFullAccess .....	920
A utilização desta política .....	920
Detalhes da política .....	920
Versão da política .....	921
Documento da política JSON .....	921
Saiba mais .....	921
AmazonRoute53ResolverReadOnlyAccess .....	922
A utilização desta política .....	922
Detalhes da política .....	922
Versão da política .....	922
Documento da política JSON .....	922
Saiba mais .....	923
AmazonS3FullAccess .....	923
A utilização desta política .....	923
Detalhes da política .....	923
Versão da política .....	923
Documento da política JSON .....	924
Saiba mais .....	924
AmazonS3ObjectLambdaExecutionRolePolicy .....	924
A utilização desta política .....	924
Detalhes da política .....	925
Versão da política .....	925
Documento da política JSON .....	925
Saiba mais .....	925
AmazonS3OutpostsFullAccess .....	926
A utilização desta política .....	926
Detalhes da política .....	926
Versão da política .....	926
Documento da política JSON .....	926
Saiba mais .....	927
AmazonS3OutpostsReadOnlyAccess .....	928
A utilização desta política .....	928
Detalhes da política .....	928
Versão da política .....	928
Documento da política JSON .....	928
Saiba mais .....	929

AmazonS3ReadOnlyAccess .....	929
A utilização desta política .....	930
Detalhes da política .....	930
Versão da política .....	930
Documento da política JSON .....	930
Saiba mais .....	931
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy .....	931
A utilização desta política .....	931
Detalhes da política .....	931
Versão da política .....	931
Documento da política JSON .....	932
Saiba mais .....	942
AmazonSageMakerCanvasAIServicesAccess .....	942
Utilização desta política .....	942
Detalhes desta política .....	942
Versão da política .....	942
Documento da política JSON .....	943
Saiba mais .....	946
AmazonSageMakerCanvasBedrockAccess .....	946
Utilização desta política .....	946
Detalhes desta política .....	946
Versão da política .....	946
Documento da política JSON .....	947
Saiba mais .....	947
AmazonSageMakerCanvasDataPrepFullAccess .....	948
Utilização desta política .....	948
Detalhes desta política .....	948
Versão da política .....	948
Documento da política JSON .....	948
Saiba mais .....	955
AmazonSageMakerCanvasDirectDeployAccess .....	956
A utilização desta política .....	956
Detalhes da política .....	956
Versão da política .....	956
Documento da política JSON .....	956
Saiba mais .....	957

AmazonSageMakerCanvasForecastAccess .....	957
A utilização desta política .....	957
Detalhes da política .....	958
Versão da política .....	958
Documento da política JSON .....	958
Saiba mais .....	959
AmazonSageMakerCanvasFullAccess .....	959
Utilização desta política .....	959
Detalhes desta política .....	959
Versão da política .....	959
Documento da política JSON .....	960
Saiba mais .....	968
AmazonSageMakerClusterInstanceRolePolicy .....	968
Utilização desta política .....	968
Detalhes desta política .....	968
Versão da política .....	968
Documento da política JSON .....	968
Saiba mais .....	970
AmazonSageMakerCoreServiceRolePolicy .....	970
A utilização desta política .....	971
Detalhes da política .....	971
Versão da política .....	971
Documento da política JSON .....	971
Saiba mais .....	972
AmazonSageMakerEdgeDeviceFleetPolicy .....	972
A utilização desta política .....	972
Detalhes da política .....	973
Versão da política .....	973
Documento da política JSON .....	973
Saiba mais .....	975
AmazonSageMakerFeatureStoreAccess .....	975
A utilização desta política .....	975
Detalhes da política .....	975
Versão da política .....	975
Documento da política JSON .....	976
Saiba mais .....	977



AmazonSageMakerFullAccess .....	977
Utilização desta política .....	977
Detalhes desta política .....	977
Versão da política .....	977
Documento da política JSON .....	978
Saiba mais .....	993
AmazonSageMakerGeospatialExecutionRole .....	993
A utilização desta política .....	994
Detalhes da política .....	994
Versão da política .....	994
Documento da política JSON .....	994
Saiba mais .....	995
AmazonSageMakerGeospatialFullAccess .....	995
A utilização desta política .....	995
Detalhes da política .....	995
Versão da política .....	996
Documento da política JSON .....	996
Saiba mais .....	996
AmazonSageMakerGroundTruthExecution .....	997
A utilização desta política .....	997
Detalhes da política .....	997
Versão da política .....	997
Documento da política JSON .....	997
Saiba mais .....	1001
AmazonSageMakerMechanicalTurkAccess .....	1001
A utilização desta política .....	1001
Detalhes da política .....	1001
Versão da política .....	1002
Documento da política JSON .....	1002
Saiba mais .....	1002
AmazonSageMakerModelGovernanceUseAccess .....	1002
A utilização desta política .....	1003
Detalhes da política .....	1003
Versão da política .....	1003
Documento da política JSON .....	1003
Saiba mais .....	1005

AmazonSageMakerModelRegistryFullAccess .....	1005
A utilização desta política .....	1005
Detalhes da política .....	1005
Versão da política .....	1006
Documento da política JSON .....	1006
Saiba mais .....	1009
AmazonSageMakerNotebooksServiceRolePolicy .....	1009
A utilização desta política .....	1009
Detalhes da política .....	1009
Versão da política .....	1009
Documento da política JSON .....	1010
Saiba mais .....	1013
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy .....	1013
A utilização desta política .....	1013
Detalhes da política .....	1013
Versão da política .....	1013
Documento da política JSON .....	1014
Saiba mais .....	1015
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy .....	1015
A utilização desta política .....	1015
Detalhes da política .....	1015
Versão da política .....	1015
Documento da política JSON .....	1016
Saiba mais .....	1019
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy .....	1019
A utilização desta política .....	1020
Detalhes da política .....	1020
Versão da política .....	1020
Documento da política JSON .....	1020
Saiba mais .....	1021
AmazonSageMakerPipelinesIntegrations .....	1021
A utilização desta política .....	1021
Detalhes da política .....	1021
Versão da política .....	1021
Documento da política JSON .....	1022
Saiba mais .....	1023

AmazonSageMakerReadOnly .....	1024
A utilização desta política .....	1024
Detalhes da política .....	1024
Versão da política .....	1024
Documento da política JSON .....	1024
Saiba mais .....	1025
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy .....	1026
A utilização desta política .....	1026
Detalhes da política .....	1026
Versão da política .....	1026
Documento da política JSON .....	1026
Saiba mais .....	1027
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy .....	1027
A utilização desta política .....	1028
Detalhes da política .....	1028
Versão da política .....	1028
Documento da política JSON .....	1028
Saiba mais .....	1035
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy .....	1035
A utilização desta política .....	1035
Detalhes da política .....	1036
Versão da política .....	1036
Documento da política JSON .....	1036
Saiba mais .....	1045
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy .....	1045
A utilização desta política .....	1046
Detalhes da política .....	1046
Versão da política .....	1046
Documento da política JSON .....	1046
Saiba mais .....	1048
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy .....	1048
A utilização desta política .....	1048
Detalhes da política .....	1048
Versão da política .....	1049
Documento da política JSON .....	1049
Saiba mais .....	1049

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy .....	1049
A utilização desta política .....	1050
Detalhes da política .....	1050
Versão da política .....	1050
Documento da política JSON .....	1050
Saiba mais .....	1051
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy .....	1051
A utilização desta política .....	1051
Detalhes da política .....	1051
Versão da política .....	1051
Documento da política JSON .....	1052
Saiba mais .....	1054
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy .....	1054
A utilização desta política .....	1054
Detalhes da política .....	1054
Versão da política .....	1055
Documento da política JSON .....	1055
Saiba mais .....	1064
AmazonSecurityLakeAdministrator .....	1065
Utilização desta política .....	1065
Detalhes desta política .....	1065
Versão da política .....	1065
Documento da política JSON .....	1065
Saiba mais .....	1076
AmazonSecurityLakeMetastoreManager .....	1077
Utilização desta política .....	1077
Detalhes desta política .....	1077
Versão da política .....	1077
Documento da política JSON .....	1077
Saiba mais .....	1079
AmazonSecurityLakePermissionsBoundary .....	1079
A utilização desta política .....	1080
Detalhes da política .....	1080
Versão da política .....	1080
Documento da política JSON .....	1080
Saiba mais .....	1083

AmazonSESEFullAccess .....	1083
A utilização desta política .....	1083
Detalhes da política .....	1084
Versão da política .....	1084
Documento da política JSON .....	1084
Saiba mais .....	1084
AmazonSESReadOnlyAccess .....	1085
A utilização desta política .....	1085
Detalhes da política .....	1085
Versão da política .....	1085
Documento da política JSON .....	1085
Saiba mais .....	1086
AmazonSNSFullAccess .....	1086
A utilização desta política .....	1086
Detalhes da política .....	1086
Versão da política .....	1086
Documento da política JSON .....	1086
Saiba mais .....	1087
AmazonSNSReadOnlyAccess .....	1087
A utilização desta política .....	1087
Detalhes da política .....	1087
Versão da política .....	1087
Documento da política JSON .....	1088
Saiba mais .....	1088
AmazonSNSRole .....	1088
A utilização desta política .....	1088
Detalhes da política .....	1089
Versão da política .....	1089
Documento da política JSON .....	1089
Saiba mais .....	1089
AmazonSQSFullAccess .....	1090
A utilização desta política .....	1090
Detalhes da política .....	1090
Versão da política .....	1090
Documento da política JSON .....	1090
Saiba mais .....	1091

AmazonSQSReadOnlyAccess .....	1091
A utilização desta política .....	1091
Detalhes da política .....	1091
Versão da política .....	1091
Documento da política JSON .....	1092
Saiba mais .....	1092
AmazonSSMAutomationApproverAccess .....	1092
A utilização desta política .....	1092
Detalhes da política .....	1093
Versão da política .....	1093
Documento da política JSON .....	1093
Saiba mais .....	1093
AmazonSSMAutomationRole .....	1094
A utilização desta política .....	1094
Detalhes da política .....	1094
Versão da política .....	1094
Documento da política JSON .....	1094
Saiba mais .....	1096
AmazonSSMDirectoryServiceAccess .....	1096
A utilização desta política .....	1096
Detalhes da política .....	1096
Versão da política .....	1096
Documento da política JSON .....	1097
Saiba mais .....	1097
AmazonSSMFullAccess .....	1097
A utilização desta política .....	1097
Detalhes da política .....	1097
Versão da política .....	1098
Documento da política JSON .....	1098
Saiba mais .....	1099
AmazonSSMMaintenanceWindowRole .....	1099
A utilização desta política .....	1099
Detalhes da política .....	1099
Versão da política .....	1100
Documento da política JSON .....	1100
Saiba mais .....	1101

AmazonSSMManagedEC2InstanceDefaultPolicy .....	1102
A utilização desta política .....	1102
Detalhes da política .....	1102
Versão da política .....	1102
Documento da política JSON .....	1102
Saiba mais .....	1103
AmazonSSMManagedInstanceCore .....	1104
A utilização desta política .....	1104
Detalhes da política .....	1104
Versão da política .....	1104
Documento da política JSON .....	1104
Saiba mais .....	1105
AmazonSSMPatchAssociation .....	1106
A utilização desta política .....	1106
Detalhes da política .....	1106
Versão da política .....	1106
Documento da política JSON .....	1106
Saiba mais .....	1107
AmazonSSMReadOnlyAccess .....	1107
A utilização desta política .....	1107
Detalhes da política .....	1107
Versão da política .....	1108
Documento da política JSON .....	1108
Saiba mais .....	1108
AmazonSSMServiceRolePolicy .....	1108
A utilização desta política .....	1109
Detalhes da política .....	1109
Versão da política .....	1109
Documento da política JSON .....	1109
Saiba mais .....	1114
AmazonSumerianFullAccess .....	1114
A utilização desta política .....	1114
Detalhes da política .....	1115
Versão da política .....	1115
Documento da política JSON .....	1115
Saiba mais .....	1115

AmazonTextractFullAccess .....	1116
A utilização desta política .....	1116
Detalhes da política .....	1116
Versão da política .....	1116
Documento da política JSON .....	1116
Saiba mais .....	1117
AmazonTextractServiceRole .....	1117
A utilização desta política .....	1117
Detalhes da política .....	1117
Versão da política .....	1117
Documento da política JSON .....	1117
Saiba mais .....	1118
AmazonTimestreamConsoleFullAccess .....	1118
A utilização desta política .....	1118
Detalhes da política .....	1118
Versão da política .....	1119
Documento da política JSON .....	1119
Saiba mais .....	1120
AmazonTimestreamFullAccess .....	1121
A utilização desta política .....	1121
Detalhes da política .....	1121
Versão da política .....	1121
Documento da política JSON .....	1121
Saiba mais .....	1122
AmazonTimestreamInfluxDBFullAccess .....	1123
Utilização desta política .....	1123
Detalhes desta política .....	1123
Versão da política .....	1123
Documento da política JSON .....	1123
Saiba mais .....	1125
AmazonTimestreamInfluxDBServiceRolePolicy .....	1125
Utilização desta política .....	1126
Detalhes desta política .....	1126
Versão da política .....	1126
Documento da política JSON .....	1126
Saiba mais .....	1129



AmazonTimestreamReadOnlyAccess .....	1129
A utilização desta política .....	1129
Detalhes da política .....	1129
Versão da política .....	1129
Documento da política JSON .....	1130
Saiba mais .....	1130
AmazonTranscribeFullAccess .....	1131
A utilização desta política .....	1131
Detalhes da política .....	1131
Versão da política .....	1131
Documento da política JSON .....	1131
Saiba mais .....	1132
AmazonTranscribeReadOnlyAccess .....	1132
A utilização desta política .....	1132
Detalhes da política .....	1132
Versão da política .....	1132
Documento da política JSON .....	1133
Saiba mais .....	1133
AmazonVPCCrossAccountNetworkInterfaceOperations .....	1133
A utilização desta política .....	1133
Detalhes da política .....	1134
Versão da política .....	1134
Documento da política JSON .....	1134
Saiba mais .....	1135
AmazonVPCFullAccess .....	1136
Utilização desta política .....	1136
Detalhes desta política .....	1136
Versão da política .....	1136
Documento da política JSON .....	1136
Saiba mais .....	1140
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy .....	1140
Utilização desta política .....	1140
Detalhes desta política .....	1141
Versão da política .....	1141
Documento da política JSON .....	1141
Saiba mais .....	1144

AmazonVPCReachabilityAnalyzerFullAccessPolicy .....	1144
Utilização desta política .....	1145
Detalhes desta política .....	1145
Versão da política .....	1145
Documento da política JSON .....	1145
Saiba mais .....	1148
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy .....	1148
A utilização desta política .....	1148
Detalhes da política .....	1149
Versão da política .....	1149
Documento da política JSON .....	1149
Saiba mais .....	1149
AmazonVPCReadOnlyAccess .....	1150
Utilização desta política .....	1150
Detalhes desta política .....	1150
Versão da política .....	1150
Documento da política JSON .....	1150
Saiba mais .....	1152
AmazonWorkDocsFullAccess .....	1152
A utilização desta política .....	1152
Detalhes da política .....	1152
Versão da política .....	1152
Documento da política JSON .....	1152
Saiba mais .....	1153
AmazonWorkDocsReadOnlyAccess .....	1153
A utilização desta política .....	1153
Detalhes da política .....	1153
Versão da política .....	1154
Documento da política JSON .....	1154
Saiba mais .....	1154
AmazonWorkMailEventsServiceRolePolicy .....	1154
A utilização desta política .....	1155
Detalhes da política .....	1155
Versão da política .....	1155
Documento da política JSON .....	1155
Saiba mais .....	1156

AmazonWorkMailFullAccess .....	1156
A utilização desta política .....	1156
Detalhes da política .....	1156
Versão da política .....	1156
Documento da política JSON .....	1156
Saiba mais .....	1158
AmazonWorkMailMessageFlowFullAccess .....	1159
A utilização desta política .....	1159
Detalhes da política .....	1159
Versão da política .....	1159
Documento da política JSON .....	1159
Saiba mais .....	1160
AmazonWorkMailMessageFlowReadOnlyAccess .....	1160
A utilização desta política .....	1160
Detalhes da política .....	1160
Versão da política .....	1160
Documento da política JSON .....	1160
Saiba mais .....	1161
AmazonWorkMailReadOnlyAccess .....	1161
A utilização desta política .....	1161
Detalhes da política .....	1161
Versão da política .....	1162
Documento da política JSON .....	1162
Saiba mais .....	1162
AmazonWorkSpacesAdmin .....	1163
A utilização desta política .....	1163
Detalhes da política .....	1163
Versão da política .....	1163
Documento da política JSON .....	1163
Saiba mais .....	1164
AmazonWorkSpacesApplicationManagerAdminAccess .....	1164
A utilização desta política .....	1164
Detalhes da política .....	1165
Versão da política .....	1165
Documento da política JSON .....	1165
Saiba mais .....	1165

AmazonWorkspacesPCAAccess .....	1166
A utilização desta política .....	1166
Detalhes da política .....	1166
Versão da política .....	1166
Documento da política JSON .....	1166
Saiba mais .....	1167
AmazonWorkSpacesSelfServiceAccess .....	1167
A utilização desta política .....	1167
Detalhes da política .....	1167
Versão da política .....	1167
Documento da política JSON .....	1168
Saiba mais .....	1168
AmazonWorkSpacesServiceAccess .....	1168
A utilização desta política .....	1168
Detalhes da política .....	1169
Versão da política .....	1169
Documento da política JSON .....	1169
Saiba mais .....	1169
AmazonWorkSpacesWebReadOnly .....	1170
A utilização desta política .....	1170
Detalhes da política .....	1170
Versão da política .....	1170
Documento da política JSON .....	1170
Saiba mais .....	1171
AmazonWorkSpacesWebServiceRolePolicy .....	1172
A utilização desta política .....	1172
Detalhes da política .....	1172
Versão da política .....	1172
Documento da política JSON .....	1172
Saiba mais .....	1175
AmazonZocaloFullAccess .....	1175
A utilização desta política .....	1175
Detalhes da política .....	1175
Versão da política .....	1175
Documento da política JSON .....	1175
Saiba mais .....	1176

AmazonZocaloReadOnlyAccess .....	1176
A utilização desta política .....	1176
Detalhes da política .....	1177
Versão da política .....	1177
Documento da política JSON .....	1177
Saiba mais .....	1177
AmplifyBackendDeployFullAccess .....	1178
Utilização desta política .....	1178
Detalhes desta política .....	1178
Versão da política .....	1178
Documento da política JSON .....	1178
Saiba mais .....	1181
APIGatewayServiceRolePolicy .....	1182
A utilização desta política .....	1182
Detalhes da política .....	1182
Versão da política .....	1182
Documento da política JSON .....	1182
Saiba mais .....	1185
AppIntegrationsServiceLinkedRolePolicy .....	1185
A utilização desta política .....	1185
Detalhes da política .....	1185
Versão da política .....	1185
Documento da política JSON .....	1185
Saiba mais .....	1187
ApplicationAutoScalingForAmazonAppStreamAccess .....	1187
A utilização desta política .....	1187
Detalhes da política .....	1187
Versão da política .....	1188
Documento da política JSON .....	1188
Saiba mais .....	1188
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy .....	1189
A utilização desta política .....	1189
Detalhes da política .....	1189
Versão da política .....	1189
Documento da política JSON .....	1189
Saiba mais .....	1191

AppRunnerNetworkingServiceRolePolicy .....	1192
A utilização desta política .....	1192
Detalhes da política .....	1192
Versão da política .....	1192
Documento da política JSON .....	1192
Saiba mais .....	1194
AppRunnerServiceRolePolicy .....	1194
A utilização desta política .....	1194
Detalhes da política .....	1194
Versão da política .....	1194
Documento da política JSON .....	1194
Saiba mais .....	1195
AutoScalingConsoleFullAccess .....	1196
A utilização desta política .....	1196
Detalhes da política .....	1196
Versão da política .....	1196
Documento da política JSON .....	1196
Saiba mais .....	1198
AutoScalingConsoleReadOnlyAccess .....	1198
A utilização desta política .....	1198
Detalhes da política .....	1198
Versão da política .....	1199
Documento da política JSON .....	1199
Saiba mais .....	1200
AutoScalingFullAccess .....	1200
A utilização desta política .....	1200
Detalhes da política .....	1200
Versão da política .....	1200
Documento da política JSON .....	1201
Saiba mais .....	1202
AutoScalingNotificationAccessRole .....	1202
A utilização desta política .....	1202
Detalhes da política .....	1202
Versão da política .....	1203
Documento da política JSON .....	1203
Saiba mais .....	1203

AutoScalingReadOnlyAccess .....	1204
A utilização desta política .....	1204
Detalhes da política .....	1204
Versão da política .....	1204
Documento da política JSON .....	1204
Saiba mais .....	1205
AutoScalingServiceRolePolicy .....	1205
Utilização desta política .....	1205
Detalhes desta política .....	1205
Versão da política .....	1205
Documento da política JSON .....	1206
Saiba mais .....	1208
AWS_ConfigRole .....	1209
Utilização desta política .....	1209
Detalhes desta política .....	1209
Versão da política .....	1209
Documento da política JSON .....	1209
Saiba mais .....	1240
AWSAccountActivityAccess .....	1240
A utilização desta política .....	1240
Detalhes da política .....	1240
Versão da política .....	1241
Documento da política JSON .....	1241
Saiba mais .....	1241
AWSAccountManagementFullAccess .....	1242
A utilização desta política .....	1242
Detalhes da política .....	1242
Versão da política .....	1242
Documento da política JSON .....	1242
Saiba mais .....	1243
AWSAccountManagementReadOnlyAccess .....	1243
A utilização desta política .....	1243
Detalhes da política .....	1243
Versão da política .....	1243
Documento da política JSON .....	1244
Saiba mais .....	1244

AWSAccountUsageReportAccess .....	1244
A utilização desta política .....	1244
Detalhes da política .....	1244
Versão da política .....	1245
Documento da política JSON .....	1245
Saiba mais .....	1245
AWSAgentlessDiscoveryService .....	1245
A utilização desta política .....	1246
Detalhes da política .....	1246
Versão da política .....	1246
Documento da política JSON .....	1246
Saiba mais .....	1248
AWSAppFabricFullAccess .....	1248
A utilização desta política .....	1248
Detalhes da política .....	1248
Versão da política .....	1249
Documento da política JSON .....	1249
Saiba mais .....	1250
AWSAppFabricReadOnlyAccess .....	1250
A utilização desta política .....	1250
Detalhes da política .....	1250
Versão da política .....	1251
Documento da política JSON .....	1251
Saiba mais .....	1251
AWSAppFabricServiceRolePolicy .....	1252
A utilização desta política .....	1252
Detalhes da política .....	1252
Versão da política .....	1252
Documento da política JSON .....	1252
Saiba mais .....	1253
AWSApplicationAutoscalingAppStreamFleetPolicy .....	1254
A utilização desta política .....	1254
Detalhes da política .....	1254
Versão da política .....	1254
Documento da política JSON .....	1254
Saiba mais .....	1255



AWSApplicationAutoscalingCassandraTablePolicy .....	1255
A utilização desta política .....	1255
Detalhes da política .....	1255
Versão da política .....	1256
Documento da política JSON .....	1256
Saiba mais .....	1256
AWSApplicationAutoscalingComprehendEndpointPolicy .....	1257
A utilização desta política .....	1257
Detalhes da política .....	1257
Versão da política .....	1257
Documento da política JSON .....	1257
Saiba mais .....	1258
AWSApplicationAutoScalingCustomResourcePolicy .....	1258
A utilização desta política .....	1258
Detalhes da política .....	1258
Versão da política .....	1258
Documento da política JSON .....	1259
Saiba mais .....	1259
AWSApplicationAutoscalingDynamoDBTablePolicy .....	1259
A utilização desta política .....	1259
Detalhes da política .....	1260
Versão da política .....	1260
Documento da política JSON .....	1260
Saiba mais .....	1260
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy .....	1261
A utilização desta política .....	1261
Detalhes da política .....	1261
Versão da política .....	1261
Documento da política JSON .....	1261
Saiba mais .....	1262
AWSApplicationAutoscalingECSServicePolicy .....	1262
A utilização desta política .....	1262
Detalhes da política .....	1262
Versão da política .....	1263
Documento da política JSON .....	1263
Saiba mais .....	1263

AWSApplicationAutoscalingElastiCacheRGPolicy .....	1263
A utilização desta política .....	1264
Detalhes da política .....	1264
Versão da política .....	1264
Documento da política JSON .....	1264
Saiba mais .....	1265
AWSApplicationAutoscalingEMRInstanceGroupPolicy .....	1265
A utilização desta política .....	1265
Detalhes da política .....	1265
Versão da política .....	1266
Documento da política JSON .....	1266
Saiba mais .....	1266
AWSApplicationAutoscalingKafkaClusterPolicy .....	1266
A utilização desta política .....	1267
Detalhes da política .....	1267
Versão da política .....	1267
Documento da política JSON .....	1267
Saiba mais .....	1268
AWSApplicationAutoscalingLambdaConcurrencyPolicy .....	1268
A utilização desta política .....	1268
Detalhes da política .....	1268
Versão da política .....	1268
Documento da política JSON .....	1269
Saiba mais .....	1269
AWSApplicationAutoscalingNeptuneClusterPolicy .....	1269
A utilização desta política .....	1269
Detalhes da política .....	1270
Versão da política .....	1270
Documento da política JSON .....	1270
Saiba mais .....	1272
AWSApplicationAutoscalingRDSClusterPolicy .....	1272
A utilização desta política .....	1272
Detalhes da política .....	1272
Versão da política .....	1272
Documento da política JSON .....	1272
Saiba mais .....	1273

AWSApplicationAutoscalingSageMakerEndpointPolicy .....	1273
A utilização desta política .....	1274
Detalhes desta política .....	1274
Versão da política .....	1274
Documento da política JSON .....	1274
Saiba mais .....	1275
AWSApplicationDiscoveryAgentAccess .....	1275
A utilização desta política .....	1275
Detalhes da política .....	1275
Versão da política .....	1276
Documento da política JSON .....	1276
Saiba mais .....	1276
AWSApplicationDiscoveryAgentlessCollectorAccess .....	1277
A utilização desta política .....	1277
Detalhes da política .....	1277
Versão da política .....	1277
Documento da política JSON .....	1277
Saiba mais .....	1278
AWSApplicationDiscoveryServiceFullAccess .....	1279
A utilização desta política .....	1279
Detalhes da política .....	1279
Versão da política .....	1279
Documento da política JSON .....	1279
Saiba mais .....	1281
AWSApplicationMigrationAgentInstallationPolicy .....	1281
A utilização desta política .....	1281
Detalhes da política .....	1281
Versão da política .....	1281
Documento da política JSON .....	1282
Saiba mais .....	1283
AWSApplicationMigrationAgentPolicy .....	1283
A utilização desta política .....	1283
Detalhes da política .....	1283
Versão da política .....	1283
Documento da política JSON .....	1284
Saiba mais .....	1284

AWSApplicationMigrationAgentPolicy_v2 .....	1285
A utilização desta política .....	1285
Detalhes da política .....	1285
Versão da política .....	1285
Documento da política JSON .....	1285
Saiba mais .....	1286
AWSApplicationMigrationConversionServerPolicy .....	1286
A utilização desta política .....	1287
Detalhes da política .....	1287
Versão da política .....	1287
Documento da política JSON .....	1287
Saiba mais .....	1288
AWSApplicationMigrationEC2Access .....	1288
A utilização desta política .....	1288
Detalhes da política .....	1288
Versão da política .....	1288
Documento da política JSON .....	1289
Saiba mais .....	1296
AWSApplicationMigrationFullAccess .....	1297
A utilização desta política .....	1297
Detalhes da política .....	1297
Versão da política .....	1297
Documento da política JSON .....	1297
Saiba mais .....	1302
AWSApplicationMigrationMGHAccess .....	1303
A utilização desta política .....	1303
Detalhes da política .....	1303
Versão da política .....	1303
Documento da política JSON .....	1303
Saiba mais .....	1304
AWSApplicationMigrationReadOnlyAccess .....	1304
A utilização desta política .....	1304
Detalhes da política .....	1304
Versão da política .....	1305
Documento da política JSON .....	1305
Saiba mais .....	1306

AWSApplicationMigrationReplicationServerPolicy .....	1306
A utilização desta política .....	1307
Detalhes da política .....	1307
Versão da política .....	1307
Documento da política JSON .....	1307
Saiba mais .....	1309
AWSApplicationMigrationServiceEc2InstancePolicy .....	1309
Utilização desta política .....	1309
Detalhes desta política .....	1309
Versão da política .....	1310
Documento da política JSON .....	1310
Saiba mais .....	1311
AWSApplicationMigrationServiceRolePolicy .....	1311
A utilização desta política .....	1311
Detalhes da política .....	1311
Versão da política .....	1312
Documento da política JSON .....	1312
Saiba mais .....	1319
AWSApplicationMigrationSSMAccess .....	1319
A utilização desta política .....	1319
Detalhes da política .....	1319
Versão da política .....	1319
Documento da política JSON .....	1320
Saiba mais .....	1321
AWSApplicationMigrationVCenterClientPolicy .....	1322
A utilização desta política .....	1322
Detalhes da política .....	1322
Versão da política .....	1322
Documento da política JSON .....	1322
Saiba mais .....	1323
AWSAppMeshEnvoyAccess .....	1323
A utilização desta política .....	1323
Detalhes da política .....	1324
Versão da política .....	1324
Documento da política JSON .....	1324
Saiba mais .....	1324

AWSAppMeshFullAccess .....	1325
A utilização desta política .....	1325
Detalhes da política .....	1325
Versão da política .....	1325
Documento da política JSON .....	1325
Saiba mais .....	1327
AWSAppMeshPreviewEnvoyAccess .....	1327
A utilização desta política .....	1327
Detalhes da política .....	1327
Versão da política .....	1327
Documento da política JSON .....	1327
Saiba mais .....	1328
AWSAppMeshPreviewServiceRolePolicy .....	1328
A utilização desta política .....	1328
Detalhes da política .....	1328
Versão da política .....	1329
Documento da política JSON .....	1329
Saiba mais .....	1329
AWSAppMeshReadOnly .....	1330
A utilização desta política .....	1330
Detalhes da política .....	1330
Versão da política .....	1330
Documento da política JSON .....	1330
Saiba mais .....	1331
AWSAppMeshServiceRolePolicy .....	1331
A utilização desta política .....	1332
Detalhes da política .....	1332
Versão da política .....	1332
Documento da política JSON .....	1332
Saiba mais .....	1333
AWSAppRunnerFullAccess .....	1333
A utilização desta política .....	1333
Detalhes da política .....	1333
Versão da política .....	1333
Documento da política JSON .....	1333
Saiba mais .....	1334

AWSAppRunnerReadOnlyAccess .....	1335
A utilização desta política .....	1335
Detalhes da política .....	1335
Versão da política .....	1335
Documento da política JSON .....	1335
Saiba mais .....	1336
AWSAppRunnerServicePolicyForECRAccess .....	1336
A utilização desta política .....	1336
Detalhes da política .....	1336
Versão da política .....	1336
Documento da política JSON .....	1337
Saiba mais .....	1337
AWSAppSyncAdministrator .....	1337
A utilização desta política .....	1337
Detalhes da política .....	1337
Versão da política .....	1338
Documento da política JSON .....	1338
Saiba mais .....	1339
AWSAppSyncInvokeFullAccess .....	1339
A utilização desta política .....	1339
Detalhes da política .....	1339
Versão da política .....	1340
Documento da política JSON .....	1340
Saiba mais .....	1340
AWSAppSyncPushToCloudWatchLogs .....	1341
A utilização desta política .....	1341
Detalhes da política .....	1341
Versão da política .....	1341
Documento da política JSON .....	1341
Saiba mais .....	1342
AWSAppSyncSchemaAuthor .....	1342
A utilização desta política .....	1342
Detalhes da política .....	1342
Versão da política .....	1342
Documento da política JSON .....	1342
Saiba mais .....	1344

AWSAppSyncServiceRolePolicy .....	1344
A utilização desta política .....	1344
Detalhes da política .....	1344
Versão da política .....	1344
Documento da política JSON .....	1344
Saiba mais .....	1345
AWSArtifactAccountSync .....	1345
A utilização desta política .....	1345
Detalhes da política .....	1345
Versão da política .....	1346
Documento da política JSON .....	1346
Saiba mais .....	1346
AWSArtifactReportsReadOnlyAccess .....	1346
Utilização desta política .....	1347
Detalhes desta política .....	1347
Versão da política .....	1347
Documento da política JSON .....	1347
Saiba mais .....	1348
AWSArtifactServiceRolePolicy .....	1348
A utilização desta política .....	1348
Detalhes da política .....	1348
Versão da política .....	1348
Documento da política JSON .....	1349
Saiba mais .....	1349
AWSAuditManagerAdministratorAccess .....	1349
A utilização desta política .....	1349
Detalhes da política .....	1349
Versão da política .....	1350
Documento da política JSON .....	1350
Saiba mais .....	1354
AWSAuditManagerServiceRolePolicy .....	1354
Utilização desta política .....	1354
Detalhes desta política .....	1354
Versão da política .....	1354
Documento da política JSON .....	1355
Saiba mais .....	1359



AWSAutoScalingPlansEC2AutoScalingPolicy .....	1359
A utilização desta política .....	1359
Detalhes da política .....	1359
Versão da política .....	1360
Documento da política JSON .....	1360
Saiba mais .....	1360
AWSBackupAuditAccess .....	1361
A utilização desta política .....	1361
Detalhes da política .....	1361
Versão da política .....	1361
Documento da política JSON .....	1361
Saiba mais .....	1363
AWSBackupDataTransferAccess .....	1363
A utilização desta política .....	1363
Detalhes da política .....	1363
Versão da política .....	1363
Documento da política JSON .....	1363
Saiba mais .....	1364
AWSBackupFullAccess .....	1364
Utilização desta política .....	1364
Detalhes desta política .....	1365
Versão da política .....	1365
Documento da política JSON .....	1365
Saiba mais .....	1375
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync .....	1375
A utilização desta política .....	1375
Detalhes da política .....	1375
Versão da política .....	1376
Documento da política JSON .....	1376
Saiba mais .....	1376
AWSBackupOperatorAccess .....	1377
A utilização desta política .....	1377
Detalhes da política .....	1377
Versão da política .....	1377
Documento da política JSON .....	1377
Saiba mais .....	1384

AWSBackupOrganizationAdminAccess .....	1384
A utilização desta política .....	1384
Detalhes da política .....	1384
Versão da política .....	1385
Documento da política JSON .....	1385
Saiba mais .....	1387
AWSBackupRestoreAccessForSAPHANA .....	1387
A utilização desta política .....	1387
Detalhes da política .....	1387
Versão da política .....	1387
Documento da política JSON .....	1388
Saiba mais .....	1388
AWSBackupServiceLinkedRolePolicyForBackup .....	1389
Utilização desta política .....	1389
Detalhes desta política .....	1389
Versão da política .....	1389
Documento da política JSON .....	1389
Saiba mais .....	1397
AWSBackupServiceLinkedRolePolicyForBackupTest .....	1397
A utilização desta política .....	1397
Detalhes da política .....	1397
Versão da política .....	1398
Documento da política JSON .....	1398
Saiba mais .....	1399
AWSBackupServiceRolePolicyForBackup .....	1399
Utilização desta política .....	1399
Detalhes desta política .....	1399
Versão da política .....	1399
Documento da política JSON .....	1399
Saiba mais .....	1410
AWSBackupServiceRolePolicyForRestores .....	1410
Utilização desta política .....	1411
Detalhes desta política .....	1411
Versão da política .....	1411
Documento da política JSON .....	1411
Saiba mais .....	1421

AWSBackupServiceRolePolicyForS3Backup .....	1421
A utilização desta política .....	1421
Detalhes da política .....	1421
Versão da política .....	1422
Documento da política JSON .....	1422
Saiba mais .....	1424
AWSBackupServiceRolePolicyForS3Restore .....	1424
A utilização desta política .....	1424
Detalhes da política .....	1424
Versão da política .....	1424
Documento da política JSON .....	1425
Saiba mais .....	1426
AWSBatchFullAccess .....	1426
A utilização desta política .....	1426
Detalhes da política .....	1426
Versão da política .....	1427
Documento da política JSON .....	1427
Saiba mais .....	1428
AWSBatchServiceEventTargetRole .....	1429
A utilização desta política .....	1429
Detalhes da política .....	1429
Versão da política .....	1429
Documento da política JSON .....	1429
Saiba mais .....	1430
AWSBatchServiceRole .....	1430
Utilização desta política .....	1430
Detalhes desta política .....	1430
Versão da política .....	1430
Documento da política JSON .....	1430
Saiba mais .....	1434
AWSBillingConductorFullAccess .....	1434
A utilização desta política .....	1434
Detalhes da política .....	1434
Versão da política .....	1434
Documento da política JSON .....	1435
Saiba mais .....	1435

AWSBillingConductorReadOnlyAccess .....	1435
A utilização desta política .....	1435
Detalhes da política .....	1436
Versão da política .....	1436
Documento da política JSON .....	1436
Saiba mais .....	1436
AWSBillingReadOnlyAccess .....	1437
Utilização desta política .....	1437
Detalhes desta política .....	1437
Versão da política .....	1437
Documento da política JSON .....	1437
Saiba mais .....	1439
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM .....	1439
A utilização desta política .....	1439
Detalhes da política .....	1439
Versão da política .....	1439
Documento da política JSON .....	1440
Saiba mais .....	1441
AWSBudgetsActionsWithAWSResourceControlAccess .....	1441
A utilização desta política .....	1441
Detalhes da política .....	1441
Versão da política .....	1441
Documento da política JSON .....	1442
Saiba mais .....	1443
AWSBudgetsReadOnlyAccess .....	1443
A utilização desta política .....	1443
Detalhes da política .....	1443
Versão da política .....	1443
Documento da política JSON .....	1444
Saiba mais .....	1444
AWSBugBustFullAccess .....	1444
A utilização desta política .....	1444
Detalhes da política .....	1445
Versão da política .....	1445
Documento da política JSON .....	1445
Saiba mais .....	1446

AWSBugBustPlayerAccess .....	1446
A utilização desta política .....	1446
Detalhes da política .....	1447
Versão da política .....	1447
Documento da política JSON .....	1447
Saiba mais .....	1448
AWSBugBustServiceRolePolicy .....	1448
A utilização desta política .....	1448
Detalhes da política .....	1448
Versão da política .....	1449
Documento da política JSON .....	1449
Saiba mais .....	1449
AWSCertificateManagerFullAccess .....	1450
A utilização desta política .....	1450
Detalhes da política .....	1450
Versão da política .....	1450
Documento da política JSON .....	1450
Saiba mais .....	1451
AWSCertificateManagerPrivateCAAuditor .....	1451
A utilização desta política .....	1451
Detalhes da política .....	1452
Versão da política .....	1452
Documento da política JSON .....	1452
Saiba mais .....	1453
AWSCertificateManagerPrivateCAFullAccess .....	1453
A utilização desta política .....	1453
Detalhes da política .....	1453
Versão da política .....	1453
Documento da política JSON .....	1454
Saiba mais .....	1454
AWSCertificateManagerPrivateCAPrivilegedUser .....	1454
A utilização desta política .....	1454
Detalhes da política .....	1454
Versão da política .....	1455
Documento da política JSON .....	1455
Saiba mais .....	1456

AWSCertificateManagerPrivateCAReadOnly .....	1456
A utilização desta política .....	1456
Detalhes da política .....	1457
Versão da política .....	1457
Documento da política JSON .....	1457
Saiba mais .....	1457
AWSCertificateManagerPrivateCAUser .....	1458
A utilização desta política .....	1458
Detalhes da política .....	1458
Versão da política .....	1458
Documento da política JSON .....	1458
Saiba mais .....	1460
AWSCertificateManagerReadOnly .....	1460
A utilização desta política .....	1460
Detalhes da política .....	1460
Versão da política .....	1460
Documento da política JSON .....	1460
Saiba mais .....	1461
AWSChatbotServiceLinkedRolePolicy .....	1461
A utilização desta política .....	1461
Detalhes da política .....	1461
Versão da política .....	1462
Documento da política JSON .....	1462
Saiba mais .....	1462
AWSCleanRoomsFullAccess .....	1463
Utilização desta política .....	1463
Detalhes desta política .....	1463
Versão da política .....	1463
Documento da política JSON .....	1463
Saiba mais .....	1468
AWSCleanRoomsFullAccessNoQuerying .....	1468
A utilização desta política .....	1468
Detalhes da política .....	1468
Versão da política .....	1468
Documento da política JSON .....	1469
Saiba mais .....	1473

---

AWSCleanRoomsMLFullAccess .....	1474
Utilização desta política .....	1474
Detalhes desta política .....	1474
Versão da política .....	1474
Documento da política JSON .....	1474
Saiba mais .....	1478
AWSCleanRoomsMLReadOnlyAccess .....	1478
Utilização desta política .....	1478
Detalhes desta política .....	1478
Versão da política .....	1478
Documento da política JSON .....	1479
Saiba mais .....	1480
AWSCleanRoomsReadOnlyAccess .....	1480
A utilização desta política .....	1480
Detalhes da política .....	1480
Versão da política .....	1480
Documento da política JSON .....	1480
Saiba mais .....	1482
AWSCloud9Administrator .....	1482
A utilização desta política .....	1482
Detalhes da política .....	1482
Versão da política .....	1482
Documento da política JSON .....	1483
Saiba mais .....	1484
AWSCloud9EnvironmentMember .....	1484
A utilização desta política .....	1484
Detalhes da política .....	1484
Versão da política .....	1485
Documento da política JSON .....	1485
Saiba mais .....	1486
AWSCloud9ServiceRolePolicy .....	1486
A utilização desta política .....	1486
Detalhes da política .....	1487
Versão da política .....	1487
Documento da política JSON .....	1487
Saiba mais .....	1489

AWSCloud9SSMInstanceProfile .....	1490
A utilização desta política .....	1490
Detalhes da política .....	1490
Versão da política .....	1490
Documento da política JSON .....	1490
Saiba mais .....	1491
AWSCloud9User .....	1491
A utilização desta política .....	1491
Detalhes da política .....	1491
Versão da política .....	1491
Documento da política JSON .....	1492
Saiba mais .....	1494
AWSCloudFormationFullAccess .....	1494
A utilização desta política .....	1494
Detalhes da política .....	1494
Versão da política .....	1495
Documento da política JSON .....	1495
Saiba mais .....	1495
AWSCloudFormationReadOnlyAccess .....	1495
A utilização desta política .....	1495
Detalhes da política .....	1496
Versão da política .....	1496
Documento da política JSON .....	1496
Saiba mais .....	1496
AWSCloudFrontLogger .....	1497
A utilização desta política .....	1497
Detalhes da política .....	1497
Versão da política .....	1497
Documento da política JSON .....	1497
Saiba mais .....	1498
AWSCloudHSMFullAccess .....	1498
A utilização desta política .....	1498
Detalhes da política .....	1498
Versão da política .....	1498
Documento da política JSON .....	1499
Saiba mais .....	1499



AWSCloudHSMReadOnlyAccess .....	1499
A utilização desta política .....	1499
Detalhes da política .....	1499
Versão da política .....	1500
Documento da política JSON .....	1500
Saiba mais .....	1500
AWSCloudHSMRole .....	1500
A utilização desta política .....	1501
Detalhes da política .....	1501
Versão da política .....	1501
Documento da política JSON .....	1501
Saiba mais .....	1502
AWSCloudMapDiscoverInstanceAccess .....	1502
A utilização desta política .....	1502
Detalhes da política .....	1502
Versão da política .....	1502
Documento da política JSON .....	1503
Saiba mais .....	1503
AWSCloudMapFullAccess .....	1503
A utilização desta política .....	1503
Detalhes da política .....	1503
Versão da política .....	1504
Documento da política JSON .....	1504
Saiba mais .....	1505
AWSCloudMapReadOnlyAccess .....	1505
A utilização desta política .....	1505
Detalhes da política .....	1505
Versão da política .....	1505
Documento da política JSON .....	1505
Saiba mais .....	1506
AWSCloudMapRegisterInstanceAccess .....	1506
A utilização desta política .....	1506
Detalhes da política .....	1506
Versão da política .....	1507
Documento da política JSON .....	1507
Saiba mais .....	1508

AWSCloudShellFullAccess .....	1508
A utilização desta política .....	1508
Detalhes da política .....	1508
Versão da política .....	1508
Documento da política JSON .....	1508
Saiba mais .....	1509
AWSCloudTrail_FullAccess .....	1509
A utilização desta política .....	1509
Detalhes da política .....	1509
Versão da política .....	1509
Documento da política JSON .....	1510
Saiba mais .....	1512
AWSCloudTrail_ReadOnlyAccess .....	1512
A utilização desta política .....	1512
Detalhes da política .....	1513
Versão da política .....	1513
Documento da política JSON .....	1513
Saiba mais .....	1513
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy .....	1514
A utilização desta política .....	1514
Detalhes da política .....	1514
Versão da política .....	1514
Documento da política JSON .....	1514
Saiba mais .....	1515
AWSCodeArtifactAdminAccess .....	1515
A utilização desta política .....	1515
Detalhes da política .....	1515
Versão da política .....	1515
Documento da política JSON .....	1516
Saiba mais .....	1516
AWSCodeArtifactReadOnlyAccess .....	1516
A utilização desta política .....	1517
Detalhes da política .....	1517
Versão da política .....	1517
Documento da política JSON .....	1517
Saiba mais .....	1518

AWSCodeBuildAdminAccess .....	1518
A utilização desta política .....	1518
Detalhes da política .....	1518
Versão da política .....	1518
Documento da política JSON .....	1519
Saiba mais .....	1522
AWSCodeBuildDeveloperAccess .....	1522
A utilização desta política .....	1522
Detalhes da política .....	1522
Versão da política .....	1523
Documento da política JSON .....	1523
Saiba mais .....	1525
AWSCodeBuildReadOnlyAccess .....	1526
A utilização desta política .....	1526
Detalhes da política .....	1526
Versão da política .....	1526
Documento da política JSON .....	1526
Saiba mais .....	1528
AWSCodeCommitFullAccess .....	1528
A utilização desta política .....	1528
Detalhes da política .....	1528
Versão da política .....	1528
Documento da política JSON .....	1528
Saiba mais .....	1533
AWSCodeCommitPowerUser .....	1533
A utilização desta política .....	1533
Detalhes da política .....	1533
Versão da política .....	1534
Documento da política JSON .....	1534
Saiba mais .....	1539
AWSCodeCommitReadOnly .....	1539
A utilização desta política .....	1539
Detalhes da política .....	1539
Versão da política .....	1539
Documento da política JSON .....	1539
Saiba mais .....	1542

AWSCodeDeployDeployerAccess .....	1542
A utilização desta política .....	1542
Detalhes da política .....	1542
Versão da política .....	1543
Documento da política JSON .....	1543
Saiba mais .....	1544
AWSCodeDeployFullAccess .....	1545
A utilização desta política .....	1545
Detalhes da política .....	1545
Versão da política .....	1545
Documento da política JSON .....	1545
Saiba mais .....	1547
AWSCodeDeployReadOnlyAccess .....	1547
A utilização desta política .....	1547
Detalhes da política .....	1547
Versão da política .....	1547
Documento da política JSON .....	1548
Saiba mais .....	1549
AWSCodeDeployRole .....	1549
A utilização desta política .....	1549
Detalhes da política .....	1549
Versão da política .....	1549
Documento da política JSON .....	1549
Saiba mais .....	1551
AWSCodeDeployRoleForCloudFormation .....	1551
A utilização desta política .....	1551
Detalhes da política .....	1551
Versão da política .....	1551
Documento da política JSON .....	1552
Saiba mais .....	1552
AWSCodeDeployRoleForECS .....	1552
A utilização desta política .....	1552
Detalhes da política .....	1553
Versão da política .....	1553
Documento da política JSON .....	1553
Saiba mais .....	1554

AWSCodeDeployRoleForECSLimited .....	1554
A utilização desta política .....	1554
Detalhes da política .....	1554
Versão da política .....	1555
Documento da política JSON .....	1555
Saiba mais .....	1557
AWSCodeDeployRoleForLambda .....	1557
A utilização desta política .....	1557
Detalhes da política .....	1557
Versão da política .....	1557
Documento da política JSON .....	1557
Saiba mais .....	1559
AWSCodeDeployRoleForLambdaLimited .....	1559
A utilização desta política .....	1559
Detalhes da política .....	1559
Versão da política .....	1559
Documento da política JSON .....	1559
Saiba mais .....	1561
AWSCodePipeline_FullAccess .....	1561
Utilização desta política .....	1561
Detalhes desta política .....	1561
Versão da política .....	1561
Documento da política JSON .....	1561
Saiba mais .....	1565
AWSCodePipeline_ReadOnlyAccess .....	1565
A utilização desta política .....	1565
Detalhes da política .....	1566
Versão da política .....	1566
Documento da política JSON .....	1566
Saiba mais .....	1567
AWSCodePipelineApproverAccess .....	1567
A utilização desta política .....	1567
Detalhes da política .....	1568
Versão da política .....	1568
Documento da política JSON .....	1568
Saiba mais .....	1568

AWSCodePipelineCustomActionAccess .....	1569
A utilização desta política .....	1569
Detalhes da política .....	1569
Versão da política .....	1569
Documento da política JSON .....	1569
Saiba mais .....	1570
AWSCodeStarFullAccess .....	1570
A utilização desta política .....	1570
Detalhes da política .....	1570
Versão da política .....	1571
Documento da política JSON .....	1571
Saiba mais .....	1572
AWSCodeStarNotificationsServiceRolePolicy .....	1572
A utilização desta política .....	1572
Detalhes da política .....	1572
Versão da política .....	1572
Documento da política JSON .....	1572
Saiba mais .....	1574
AWSCodeStarServiceRole .....	1574
A utilização desta política .....	1574
Detalhes da política .....	1574
Versão da política .....	1574
Documento da política JSON .....	1574
Saiba mais .....	1579
AWSCompromisedKeyQuarantine .....	1579
A utilização desta política .....	1580
Detalhes da política .....	1580
Versão da política .....	1580
Documento da política JSON .....	1580
Saiba mais .....	1581
AWSCompromisedKeyQuarantineV2 .....	1581
A utilização desta política .....	1582
Detalhes da política .....	1582
Versão da política .....	1582
Documento da política JSON .....	1582
Saiba mais .....	1584

AWSConfigMultiAccountSetupPolicy .....	1584
A utilização desta política .....	1584
Detalhes da política .....	1584
Versão da política .....	1585
Documento da política JSON .....	1585
Saiba mais .....	1587
AWSConfigRemediationServiceRolePolicy .....	1587
A utilização desta política .....	1587
Detalhes da política .....	1587
Versão da política .....	1587
Documento da política JSON .....	1587
Saiba mais .....	1588
AWSConfigRoleForOrganizations .....	1588
A utilização desta política .....	1588
Detalhes da política .....	1589
Versão da política .....	1589
Documento da política JSON .....	1589
Saiba mais .....	1589
AWSConfigRulesExecutionRole .....	1590
A utilização desta política .....	1590
Detalhes da política .....	1590
Versão da política .....	1590
Documento da política JSON .....	1590
Saiba mais .....	1591
AWSConfigServiceRolePolicy .....	1591
Utilização desta política .....	1591
Detalhes desta política .....	1592
Versão da política .....	1592
Documento da política JSON .....	1592
Saiba mais .....	1623
AWSConfigUserAccess .....	1624
A utilização desta política .....	1624
Detalhes da política .....	1624
Versão da política .....	1624
Documento da política JSON .....	1624
Saiba mais .....	1625

AWSCongressionalAccountServiceRolePolicy .....	1625
Utilização desta política .....	1625
Detalhes desta política .....	1625
Versão da política .....	1626
Documento da política JSON .....	1626
Saiba mais .....	1628
AWSCongressionalAccountServiceRolePolicy .....	1628
A utilização desta política .....	1628
Detalhes da política .....	1628
Versão da política .....	1628
Documento da política JSON .....	1629
Saiba mais .....	1630
AWSCongressionalServiceRolePolicy .....	1630
A utilização desta política .....	1631
Detalhes da política .....	1631
Versão da política .....	1631
Documento da política JSON .....	1631
Saiba mais .....	1636
AWSCongressionalServiceRolePolicy .....	1636
A utilização desta política .....	1636
Detalhes da política .....	1636
Versão da política .....	1636
Documento da política JSON .....	1637
Saiba mais .....	1638
AWSCongressionalServiceRolePolicy .....	1638
A utilização desta política .....	1638
Detalhes da política .....	1638
Versão da política .....	1638
Documento da política JSON .....	1638
Saiba mais .....	1642
AWSCongressionalServiceRolePolicy .....	1642
A utilização desta política .....	1642
Detalhes da política .....	1642
Versão da política .....	1642
Documento da política JSON .....	1643
Saiba mais .....	1646



AWSDataExchangeReadOnly .....	1646
A utilização desta política .....	1647
Detalhes da política .....	1647
Versão da política .....	1647
Documento da política JSON .....	1647
Saiba mais .....	1648
AWSDataExchangeSubscriberFullAccess .....	1648
A utilização desta política .....	1648
Detalhes da política .....	1648
Versão da política .....	1649
Documento da política JSON .....	1649
Saiba mais .....	1651
AWSDataLifecycleManagerServiceRole .....	1651
A utilização desta política .....	1651
Detalhes da política .....	1651
Versão da política .....	1651
Documento da política JSON .....	1652
Saiba mais .....	1653
AWSDataLifecycleManagerServiceRoleForAMIManagement .....	1653
A utilização desta política .....	1653
Detalhes da política .....	1653
Versão da política .....	1654
Documento da política JSON .....	1654
Saiba mais .....	1655
AWSDataLifecycleManagerSSMFullAccess .....	1655
Utilização desta política .....	1655
Detalhes desta política .....	1655
Versão da política .....	1656
Documento da política JSON .....	1656
Saiba mais .....	1657
AWSDataPipeline_FullAccess .....	1658
A utilização desta política .....	1658
Detalhes da política .....	1658
Versão da política .....	1658
Documento da política JSON .....	1658
Saiba mais .....	1659

AWSDatapipeline_PowerUser .....	1659
A utilização desta política .....	1659
Detalhes da política .....	1660
Versão da política .....	1660
Documento da política JSON .....	1660
Saiba mais .....	1661
AWSDatasyncDiscoveryServiceRolePolicy .....	1661
A utilização desta política .....	1661
Detalhes da política .....	1661
Versão da política .....	1662
Documento da política JSON .....	1662
Saiba mais .....	1663
AWSDatasyncFullAccess .....	1663
Utilização desta política .....	1663
Detalhes desta política .....	1663
Versão da política .....	1663
Documento da política JSON .....	1664
Saiba mais .....	1665
AWSDatasyncReadOnlyAccess .....	1665
A utilização desta política .....	1665
Detalhes da política .....	1665
Versão da política .....	1666
Documento da política JSON .....	1666
Saiba mais .....	1666
AWSDeepLensLambdaFunctionAccessPolicy .....	1667
A utilização desta política .....	1667
Detalhes da política .....	1667
Versão da política .....	1667
Documento da política JSON .....	1667
Saiba mais .....	1669
AWSDeepLensServiceRolePolicy .....	1669
A utilização desta política .....	1669
Detalhes da política .....	1669
Versão da política .....	1669
Documento da política JSON .....	1670
Saiba mais .....	1677

AWSDeeperRacerAccountAdminAccess .....	1677
A utilização desta política .....	1677
Detalhes da política .....	1677
Versão da política .....	1677
Documento da política JSON .....	1678
Saiba mais .....	1678
AWSDeeperRacerCloudFormationAccessPolicy .....	1678
A utilização desta política .....	1679
Detalhes da política .....	1679
Versão da política .....	1679
Documento da política JSON .....	1679
Saiba mais .....	1682
AWSDeeperRacerDefaultMultiUserAccess .....	1682
A utilização desta política .....	1682
Detalhes da política .....	1682
Versão da política .....	1683
Documento da política JSON .....	1683
Saiba mais .....	1684
AWSDeeperRacerFullAccess .....	1685
A utilização desta política .....	1685
Detalhes da política .....	1685
Versão da política .....	1685
Documento da política JSON .....	1685
Saiba mais .....	1686
AWSDeeperRacerRoboMakerAccessPolicy .....	1686
A utilização desta política .....	1687
Detalhes da política .....	1687
Versão da política .....	1687
Documento da política JSON .....	1687
Saiba mais .....	1689
AWSDeeperRacerServiceRolePolicy .....	1689
A utilização desta política .....	1689
Detalhes da política .....	1689
Versão da política .....	1690
Documento da política JSON .....	1690
Saiba mais .....	1693

AWSDenyAll .....	1693
Utilização desta política .....	1693
Detalhes desta política .....	1693
Versão da política .....	1694
Documento da política JSON .....	1694
Saiba mais .....	1694
AWSDeviceFarmFullAccess .....	1694
A utilização desta política .....	1695
Detalhes da política .....	1695
Versão da política .....	1695
Documento da política JSON .....	1695
Saiba mais .....	1695
AWSDeviceFarmServiceRolePolicy .....	1696
A utilização desta política .....	1696
Detalhes da política .....	1696
Versão da política .....	1696
Documento da política JSON .....	1696
Saiba mais .....	1698
AWSDeviceFarmTestGridServiceRolePolicy .....	1699
A utilização desta política .....	1699
Detalhes da política .....	1699
Versão da política .....	1699
Documento da política JSON .....	1699
Saiba mais .....	1701
AWSDirectConnectFullAccess .....	1702
A utilização desta política .....	1702
Detalhes da política .....	1702
Versão da política .....	1702
Documento da política JSON .....	1702
Saiba mais .....	1703
AWSDirectConnectReadOnlyAccess .....	1703
A utilização desta política .....	1703
Detalhes da política .....	1703
Versão da política .....	1703
Documento da política JSON .....	1703
Saiba mais .....	1704

AWSDirectConnectServiceRolePolicy .....	1704
A utilização desta política .....	1704
Detalhes da política .....	1704
Versão da política .....	1705
Documento da política JSON .....	1705
Saiba mais .....	1705
AWSDirectoryServiceFullAccess .....	1706
A utilização desta política .....	1706
Detalhes da política .....	1706
Versão da política .....	1706
Documento da política JSON .....	1706
Saiba mais .....	1708
AWSDirectoryServiceReadOnlyAccess .....	1708
A utilização desta política .....	1708
Detalhes da política .....	1708
Versão da política .....	1709
Documento da política JSON .....	1709
Saiba mais .....	1709
AWSDiscoveryContinuousExportFirehosePolicy .....	1710
A utilização desta política .....	1710
Detalhes da política .....	1710
Versão da política .....	1710
Documento da política JSON .....	1710
Saiba mais .....	1711
AWSDMSFleetAdvisorServiceRolePolicy .....	1712
A utilização desta política .....	1712
Detalhes da política .....	1712
Versão da política .....	1712
Documento da política JSON .....	1712
Saiba mais .....	1713
AWSDMSServerlessServiceRolePolicy .....	1713
A utilização desta política .....	1713
Detalhes da política .....	1713
Versão da política .....	1713
Documento da política JSON .....	1714
Saiba mais .....	1715

AWSEC2CapacityReservationFleetRolePolicy .....	1715
A utilização desta política .....	1715
Detalhes da política .....	1715
Versão da política .....	1716
Documento da política JSON .....	1716
Saiba mais .....	1717
AWSEC2FleetServiceRolePolicy .....	1717
A utilização desta política .....	1717
Detalhes da política .....	1717
Versão da política .....	1718
Documento da política JSON .....	1718
Saiba mais .....	1720
AWSEC2SpotFleetServiceRolePolicy .....	1720
A utilização desta política .....	1720
Detalhes da política .....	1720
Versão da política .....	1720
Documento da política JSON .....	1721
Saiba mais .....	1723
AWSEC2SpotServiceRolePolicy .....	1723
A utilização desta política .....	1723
Detalhes da política .....	1723
Versão da política .....	1723
Documento da política JSON .....	1723
Saiba mais .....	1725
AWSECRPullThroughCache_ServiceRolePolicy .....	1725
Utilização desta política .....	1725
Detalhes desta política .....	1725
Versão da política .....	1726
Documento da política JSON .....	1726
Saiba mais .....	1727
AWSElasticBeanstalkCustomPlatformforEC2Role .....	1727
A utilização desta política .....	1727
Detalhes da política .....	1727
Versão da política .....	1727
Documento da política JSON .....	1727
Saiba mais .....	1729

AWSElasticBeanstalkEnhancedHealth .....	1729
A utilização desta política .....	1729
Detalhes da política .....	1730
Versão da política .....	1730
Documento da política JSON .....	1730
Saiba mais .....	1731
AWSElasticBeanstalkMaintenance .....	1731
A utilização desta política .....	1731
Detalhes da política .....	1731
Versão da política .....	1732
Documento da política JSON .....	1732
Saiba mais .....	1733
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy .....	1733
A utilização desta política .....	1733
Detalhes da política .....	1733
Versão da política .....	1733
Documento da política JSON .....	1734
Saiba mais .....	1740
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy .....	1741
A utilização desta política .....	1741
Detalhes da política .....	1741
Versão da política .....	1741
Documento da política JSON .....	1741
Saiba mais .....	1747
AWSElasticBeanstalkMulticontainerDocker .....	1747
A utilização desta política .....	1747
Detalhes da política .....	1747
Versão da política .....	1747
Documento da política JSON .....	1747
Saiba mais .....	1748
AWSElasticBeanstalkReadOnly .....	1749
A utilização desta política .....	1749
Detalhes da política .....	1749
Versão da política .....	1749
Documento da política JSON .....	1749
Saiba mais .....	1751

AWSElasticBeanstalkRoleCore .....	1752
A utilização desta política .....	1752
Detalhes da política .....	1752
Versão da política .....	1752
Documento da política JSON .....	1752
Saiba mais .....	1757
AWSElasticBeanstalkRoleCWL .....	1757
A utilização desta política .....	1757
Detalhes da política .....	1758
Versão da política .....	1758
Documento da política JSON .....	1758
Saiba mais .....	1758
AWSElasticBeanstalkRoleECS .....	1759
A utilização desta política .....	1759
Detalhes da política .....	1759
Versão da política .....	1759
Documento da política JSON .....	1759
Saiba mais .....	1760
AWSElasticBeanstalkRoleRDS .....	1760
A utilização desta política .....	1761
Detalhes da política .....	1761
Versão da política .....	1761
Documento da política JSON .....	1761
Saiba mais .....	1762
AWSElasticBeanstalkRoleSNS .....	1762
A utilização desta política .....	1762
Detalhes da política .....	1762
Versão da política .....	1762
Documento da política JSON .....	1763
Saiba mais .....	1763
AWSElasticBeanstalkRoleWorkerTier .....	1764
A utilização desta política .....	1764
Detalhes da política .....	1764
Versão da política .....	1764
Documento da política JSON .....	1764
Saiba mais .....	1765



AWSElasticBeanstalkService .....	1765
A utilização desta política .....	1765
Detalhes da política .....	1766
Versão da política .....	1766
Documento da política JSON .....	1766
Saiba mais .....	1770
AWSElasticBeanstalkServiceRolePolicy .....	1771
A utilização desta política .....	1771
Detalhes da política .....	1771
Versão da política .....	1771
Documento da política JSON .....	1771
Saiba mais .....	1773
AWSElasticBeanstalkWebTier .....	1773
A utilização desta política .....	1773
Detalhes da política .....	1773
Versão da política .....	1773
Documento da política JSON .....	1773
Saiba mais .....	1775
AWSElasticBeanstalkWorkerTier .....	1775
A utilização desta política .....	1775
Detalhes da política .....	1775
Versão da política .....	1776
Documento da política JSON .....	1776
Saiba mais .....	1778
AWSElasticDisasterRecoveryAgentInstallationPolicy .....	1778
Utilização desta política .....	1778
Detalhes desta política .....	1778
Versão da política .....	1779
Documento da política JSON .....	1779
Saiba mais .....	1780
AWSElasticDisasterRecoveryAgentPolicy .....	1781
Utilização desta política .....	1781
Detalhes desta política .....	1781
Versão da política .....	1781
Documento da política JSON .....	1781
Saiba mais .....	1782

AWSElasticDisasterRecoveryConsoleFullAccess .....	1782
A utilização desta política .....	1783
Detalhes da política .....	1783
Versão da política .....	1783
Documento da política JSON .....	1783
Saiba mais .....	1793
AWSElasticDisasterRecoveryConsoleFullAccess_v2 .....	1793
Utilização desta política .....	1793
Detalhes desta política .....	1793
Versão da política .....	1794
Documento da política JSON .....	1794
Saiba mais .....	1806
AWSElasticDisasterRecoveryConversionServerPolicy .....	1807
Utilização desta política .....	1807
Detalhes desta política .....	1807
Versão da política .....	1807
Documento da política JSON .....	1807
Saiba mais .....	1808
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy .....	1808
Utilização desta política .....	1809
Detalhes desta política .....	1809
Versão da política .....	1809
Documento da política JSON .....	1809
Saiba mais .....	1810
AWSElasticDisasterRecoveryEc2InstancePolicy .....	1810
Utilização desta política .....	1810
Detalhes desta política .....	1811
Versão da política .....	1811
Documento da política JSON .....	1811
Saiba mais .....	1813
AWSElasticDisasterRecoveryFailbackInstallationPolicy .....	1813
Utilização desta política .....	1813
Detalhes desta política .....	1814
Versão da política .....	1814
Documento da política JSON .....	1814
Saiba mais .....	1815

AWSElasticDisasterRecoveryFailbackPolicy .....	1815
Utilização desta política .....	1815
Detalhes desta política .....	1815
Versão da política .....	1816
Documento da política JSON .....	1816
Saiba mais .....	1817
AWSElasticDisasterRecoveryLaunchActionsPolicy .....	1817
A utilização desta política .....	1817
Detalhes da política .....	1818
Versão da política .....	1818
Documento da política JSON .....	1818
Saiba mais .....	1824
AWSElasticDisasterRecoveryNetworkReplicationPolicy .....	1824
Utilização desta política .....	1824
Detalhes desta política .....	1824
Versão da política .....	1825
Documento da política JSON .....	1825
Saiba mais .....	1826
AWSElasticDisasterRecoveryReadOnlyAccess .....	1826
Utilização desta política .....	1826
Detalhes desta política .....	1826
Versão da política .....	1826
Documento da política JSON .....	1827
Saiba mais .....	1829
AWSElasticDisasterRecoveryRecoveryInstancePolicy .....	1829
Utilização desta política .....	1829
Detalhes desta política .....	1829
Versão da política .....	1830
Documento da política JSON .....	1830
Saiba mais .....	1832
AWSElasticDisasterRecoveryReplicationServerPolicy .....	1833
Utilização desta política .....	1833
Detalhes desta política .....	1833
Versão da política .....	1833
Documento da política JSON .....	1833
Saiba mais .....	1836

AWSElasticDisasterRecoveryServiceRolePolicy .....	1836
Utilização desta política .....	1836
Detalhes desta política .....	1836
Versão da política .....	1836
Documento da política JSON .....	1837
Saiba mais .....	1845
AWSElasticDisasterRecoveryStagingAccountPolicy .....	1845
Utilização desta política .....	1845
Detalhes desta política .....	1845
Versão da política .....	1846
Documento da política JSON .....	1846
Saiba mais .....	1847
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 .....	1847
Utilização desta política .....	1847
Detalhes desta política .....	1847
Versão da política .....	1848
Documento da política JSON .....	1848
Saiba mais .....	1849
AWSElasticLoadBalancingClassicServiceRolePolicy .....	1849
A utilização desta política .....	1849
Detalhes da política .....	1849
Versão da política .....	1850
Documento da política JSON .....	1850
Saiba mais .....	1851
AWSElasticLoadBalancingServiceRolePolicy .....	1851
A utilização desta política .....	1851
Detalhes da política .....	1851
Versão da política .....	1851
Documento da política JSON .....	1851
Saiba mais .....	1853
AWSElementalMediaConvertFullAccess .....	1853
A utilização desta política .....	1853
Detalhes da política .....	1853
Versão da política .....	1853
Documento da política JSON .....	1853
Saiba mais .....	1854

AWSElementalMediaConvertReadOnly .....	1854
A utilização desta política .....	1854
Detalhes da política .....	1855
Versão da política .....	1855
Documento da política JSON .....	1855
Saiba mais .....	1855
AWSElementalMediaLiveFullAccess .....	1856
A utilização desta política .....	1856
Detalhes da política .....	1856
Versão da política .....	1856
Documento da política JSON .....	1856
Saiba mais .....	1857
AWSElementalMediaLiveReadOnly .....	1857
A utilização desta política .....	1857
Detalhes da política .....	1857
Versão da política .....	1857
Documento da política JSON .....	1857
Saiba mais .....	1858
AWSElementalMediaPackageFullAccess .....	1858
A utilização desta política .....	1858
Detalhes da política .....	1858
Versão da política .....	1858
Documento da política JSON .....	1859
Saiba mais .....	1859
AWSElementalMediaPackageReadOnly .....	1859
A utilização desta política .....	1859
Detalhes da política .....	1859
Versão da política .....	1860
Documento da política JSON .....	1860
Saiba mais .....	1860
AWSElementalMediaPackageV2FullAccess .....	1860
A utilização desta política .....	1860
Detalhes da política .....	1861
Versão da política .....	1861
Documento da política JSON .....	1861
Saiba mais .....	1861

AWSElementalMediaPackageV2ReadOnly .....	1862
A utilização desta política .....	1862
Detalhes da política .....	1862
Versão da política .....	1862
Documento da política JSON .....	1862
Saiba mais .....	1863
AWSElementalMediaStoreFullAccess .....	1863
A utilização desta política .....	1863
Detalhes da política .....	1863
Versão da política .....	1863
Documento da política JSON .....	1863
Saiba mais .....	1864
AWSElementalMediaStoreReadOnly .....	1864
A utilização desta política .....	1864
Detalhes da política .....	1864
Versão da política .....	1865
Documento da política JSON .....	1865
Saiba mais .....	1865
AWSElementalMediaTailorFullAccess .....	1866
A utilização desta política .....	1866
Detalhes da política .....	1866
Versão da política .....	1866
Documento da política JSON .....	1866
Saiba mais .....	1866
AWSElementalMediaTailorReadOnly .....	1867
A utilização desta política .....	1867
Detalhes da política .....	1867
Versão da política .....	1867
Documento da política JSON .....	1867
Saiba mais .....	1868
AWSEnhancedClassicNetworkingMangementPolicy .....	1868
A utilização desta política .....	1868
Detalhes da política .....	1868
Versão da política .....	1868
Documento da política JSON .....	1869
Saiba mais .....	1869

AWSEntityResolutionConsoleFullAccess .....	1869
A utilização desta política .....	1869
Detalhes da política .....	1869
Versão da política .....	1870
Documento da política JSON .....	1870
Saiba mais .....	1873
AWSEntityResolutionConsoleReadOnlyAccess .....	1873
A utilização desta política .....	1873
Detalhes da política .....	1873
Versão da política .....	1873
Documento da política JSON .....	1873
Saiba mais .....	1874
AWSFaultInjectionSimulatorEC2Access .....	1874
Utilização desta política .....	1874
Detalhes desta política .....	1874
Versão da política .....	1875
Documento da política JSON .....	1875
Saiba mais .....	1876
AWSFaultInjectionSimulatorECSAccess .....	1877
Utilização desta política .....	1877
Detalhes desta política .....	1877
Versão da política .....	1877
Documento da política JSON .....	1877
Saiba mais .....	1879
AWSFaultInjectionSimulatorEKSAccess .....	1879
Utilização desta política .....	1879
Detalhes desta política .....	1880
Versão da política .....	1880
Documento da política JSON .....	1880
Saiba mais .....	1881
AWSFaultInjectionSimulatorNetworkAccess .....	1881
Utilização desta política .....	1882
Detalhes desta política .....	1882
Versão da política .....	1882
Documento da política JSON .....	1882
Saiba mais .....	1889

AWSFaultInjectionSimulatorRDSAccess .....	1889
Utilização desta política .....	1889
Detalhes desta política .....	1890
Versão da política .....	1890
Documento da política JSON .....	1890
Saiba mais .....	1891
AWSFaultInjectionSimulatorSSMAccess .....	1891
A utilização desta política .....	1892
Detalhes da política .....	1892
Versão da política .....	1892
Documento da política JSON .....	1892
Saiba mais .....	1893
AWSFinSpaceServiceRolePolicy .....	1894
A utilização desta política .....	1894
Detalhes desta política .....	1894
Versão da política .....	1894
Documento da política JSON .....	1894
Saiba mais .....	1895
AWSFMAdminFullAccess .....	1895
A utilização desta política .....	1895
Detalhes da política .....	1895
Versão da política .....	1895
Documento da política JSON .....	1896
Saiba mais .....	1897
AWSFMAdminReadOnlyAccess .....	1898
A utilização desta política .....	1898
Detalhes da política .....	1898
Versão da política .....	1898
Documento da política JSON .....	1898
Saiba mais .....	1900
AWSFMMemberReadOnlyAccess .....	1900
A utilização desta política .....	1900
Detalhes da política .....	1900
Versão da política .....	1900
Documento da política JSON .....	1901
Saiba mais .....	1901



AWSForWordPressPluginPolicy .....	1901
A utilização desta política .....	1902
Detalhes da política .....	1902
Versão da política .....	1902
Documento da política JSON .....	1902
Saiba mais .....	1904
AWSGitSyncServiceRolePolicy .....	1904
Utilização desta política .....	1904
Detalhes desta política .....	1904
Versão da política .....	1905
Documento da política JSON .....	1905
Saiba mais .....	1905
AWSGlobalAcceleratorSLRPolicy .....	1905
A utilização desta política .....	1906
Detalhes da política .....	1906
Versão da política .....	1906
Documento da política JSON .....	1906
Saiba mais .....	1908
AWSGlueConsoleFullAccess .....	1908
A utilização desta política .....	1908
Detalhes da política .....	1908
Versão da política .....	1908
Documento da política JSON .....	1908
Saiba mais .....	1913
AWSGlueConsoleSageMakerNotebookFullAccess .....	1913
A utilização desta política .....	1913
Detalhes da política .....	1913
Versão da política .....	1913
Documento da política JSON .....	1913
Saiba mais .....	1919
AwsGlueDataBrewFullAccessPolicy .....	1919
A utilização desta política .....	1919
Detalhes da política .....	1919
Versão da política .....	1919
Documento da política JSON .....	1920
Saiba mais .....	1925

AWSGlueDataBrewServiceRole .....	1925
Utilização desta política .....	1925
Detalhes desta política .....	1925
Versão da política .....	1925
Documento da política JSON .....	1926
Saiba mais .....	1928
AWSGlueSchemaRegistryFullAccess .....	1929
A utilização desta política .....	1929
Detalhes da política .....	1929
Versão da política .....	1929
Documento da política JSON .....	1929
Saiba mais .....	1930
AWSGlueSchemaRegistryReadOnlyAccess .....	1931
A utilização desta política .....	1931
Detalhes da política .....	1931
Versão da política .....	1931
Documento da política JSON .....	1931
Saiba mais .....	1932
AWSGlueServiceNotebookRole .....	1932
A utilização desta política .....	1932
Detalhes da política .....	1932
Versão da política .....	1933
Documento da política JSON .....	1933
Saiba mais .....	1935
AWSGlueServiceRole .....	1935
A utilização desta política .....	1935
Detalhes da política .....	1935
Versão da política .....	1936
Documento da política JSON .....	1936
Saiba mais .....	1938
AwsGlueSessionUserRestrictedNotebookPolicy .....	1938
Utilização desta política .....	1939
Detalhes desta política .....	1939
Versão da política .....	1939
Documento da política JSON .....	1939
Saiba mais .....	1942

AwsGlueSessionUserRestrictedNotebookServiceRole .....	1942
A utilização desta política .....	1942
Detalhes da política .....	1942
Versão da política .....	1942
Documento da política JSON .....	1943
Saiba mais .....	1946
AwsGlueSessionUserRestrictedPolicy .....	1946
A utilização desta política .....	1947
Detalhes da política .....	1947
Versão da política .....	1947
Documento da política JSON .....	1947
Saiba mais .....	1949
AwsGlueSessionUserRestrictedServiceRole .....	1950
A utilização desta política .....	1950
Detalhes da política .....	1950
Versão da política .....	1950
Documento da política JSON .....	1950
Saiba mais .....	1954
AWSGrafanaAccountAdministrator .....	1954
A utilização desta política .....	1954
Detalhes da política .....	1954
Versão da política .....	1955
Documento da política JSON .....	1955
Saiba mais .....	1956
AWSGrafanaConsoleReadOnlyAccess .....	1956
A utilização desta política .....	1956
Detalhes da política .....	1956
Versão da política .....	1956
Documento da política JSON .....	1957
Saiba mais .....	1957
AWSGrafanaWorkspacePermissionManagement .....	1957
A utilização desta política .....	1957
Detalhes da política .....	1957
Versão da política .....	1958
Documento da política JSON .....	1958
Saiba mais .....	1959

AWSGrafanaWorkspacePermissionManagementV2 .....	1959
Utilização desta política .....	1959
Detalhes desta política .....	1959
Versão da política .....	1960
Documento da política JSON .....	1960
Saiba mais .....	1961
AWSGreengrassFullAccess .....	1961
A utilização desta política .....	1961
Detalhes da política .....	1961
Versão da política .....	1961
Documento da política JSON .....	1962
Saiba mais .....	1962
AWSGreengrassReadOnlyAccess .....	1962
A utilização desta política .....	1962
Detalhes da política .....	1962
Versão da política .....	1963
Documento da política JSON .....	1963
Saiba mais .....	1963
AWSGreengrassResourceAccessRolePolicy .....	1964
A utilização desta política .....	1964
Detalhes da política .....	1964
Versão da política .....	1964
Documento da política JSON .....	1964
Saiba mais .....	1967
AWSGroundStationAgentInstancePolicy .....	1967
A utilização desta política .....	1967
Detalhes da política .....	1967
Versão da política .....	1967
Documento da política JSON .....	1967
Saiba mais .....	1968
AWSHealth_EventProcessorServiceRolePolicy .....	1968
A utilização desta política .....	1968
Detalhes da política .....	1968
Versão da política .....	1969
Documento da política JSON .....	1969
Saiba mais .....	1970

AWSHealthFullAccess .....	1970
A utilização desta política .....	1970
Detalhes da política .....	1970
Versão da política .....	1970
Documento da política JSON .....	1970
Saiba mais .....	1971
AWSHealthImagingFullAccess .....	1972
A utilização desta política .....	1972
Detalhes da política .....	1972
Versão da política .....	1972
Documento da política JSON .....	1972
Saiba mais .....	1973
AWSHealthImagingReadOnlyAccess .....	1973
A utilização desta política .....	1973
Detalhes da política .....	1973
Versão da política .....	1973
Documento da política JSON .....	1974
Saiba mais .....	1974
AWSIAMIdentityCenterAllowListForIdentityContext .....	1975
Utilização desta política .....	1975
Detalhes desta política .....	1975
Versão da política .....	1975
Documento da política JSON .....	1975
Saiba mais .....	1977
AWSIdentitySyncFullAccess .....	1977
A utilização desta política .....	1977
Detalhes da política .....	1978
Versão da política .....	1978
Documento da política JSON .....	1978
Saiba mais .....	1979
AWSIdentitySyncReadOnlyAccess .....	1979
A utilização desta política .....	1979
Detalhes da política .....	1979
Versão da política .....	1979
Documento da política JSON .....	1980
Saiba mais .....	1980

AWSImageBuilderFullAccess .....	1980
A utilização desta política .....	1980
Detalhes da política .....	1981
Versão da política .....	1981
Documento da política JSON .....	1981
Saiba mais .....	1984
AWSImageBuilderReadOnlyAccess .....	1984
A utilização desta política .....	1984
Detalhes da política .....	1984
Versão da política .....	1984
Documento da política JSON .....	1984
Saiba mais .....	1985
AWSImportExportFullAccess .....	1985
A utilização desta política .....	1985
Detalhes da política .....	1986
Versão da política .....	1986
Documento da política JSON .....	1986
Saiba mais .....	1986
AWSImportExportReadOnlyAccess .....	1987
A utilização desta política .....	1987
Detalhes da política .....	1987
Versão da política .....	1987
Documento da política JSON .....	1987
Saiba mais .....	1988
AWSIncidentManagerIncidentAccessServiceRolePolicy .....	1988
Utilização desta política .....	1988
Detalhes desta política .....	1988
Versão da política .....	1988
Documento da política JSON .....	1989
Saiba mais .....	1989
AWSIncidentManagerResolverAccess .....	1989
A utilização desta política .....	1989
Detalhes da política .....	1990
Versão da política .....	1990
Documento da política JSON .....	1990
Saiba mais .....	1991

AWSIncidentManagerServiceRolePolicy .....	1991
A utilização desta política .....	1991
Detalhes da política .....	1991
Versão da política .....	1992
Documento da política JSON .....	1992
Saiba mais .....	1993
AWSIoT1ClickFullAccess .....	1993
A utilização desta política .....	1993
Detalhes da política .....	1993
Versão da política .....	1994
Documento da política JSON .....	1994
Saiba mais .....	1994
AWSIoT1ClickReadOnlyAccess .....	1994
A utilização desta política .....	1994
Detalhes da política .....	1995
Versão da política .....	1995
Documento da política JSON .....	1995
Saiba mais .....	1995
AWSIoTAnalyticsFullAccess .....	1996
A utilização desta política .....	1996
Detalhes da política .....	1996
Versão da política .....	1996
Documento da política JSON .....	1996
Saiba mais .....	1997
AWSIoTAnalyticsReadOnlyAccess .....	1997
A utilização desta política .....	1997
Detalhes da política .....	1997
Versão da política .....	1997
Documento da política JSON .....	1998
Saiba mais .....	1998
AWSIoTConfigAccess .....	1998
A utilização desta política .....	1998
Detalhes da política .....	1998
Versão da política .....	1999
Documento da política JSON .....	1999
Saiba mais .....	2003

AWSIoTConfigReadOnlyAccess .....	2003
A utilização desta política .....	2003
Detalhes da política .....	2003
Versão da política .....	2003
Documento da política JSON .....	2003
Saiba mais .....	2005
AWSIoTDataAccess .....	2006
A utilização desta política .....	2006
Detalhes da política .....	2006
Versão da política .....	2006
Documento da política JSON .....	2006
Saiba mais .....	2007
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction .....	2007
A utilização desta política .....	2007
Detalhes da política .....	2007
Versão da política .....	2008
Documento da política JSON .....	2008
Saiba mais .....	2008
AWSIoTDeviceDefenderAudit .....	2008
A utilização desta política .....	2009
Detalhes da política .....	2009
Versão da política .....	2009
Documento da política JSON .....	2009
Saiba mais .....	2010
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction .....	2010
A utilização desta política .....	2010
Detalhes da política .....	2010
Versão da política .....	2011
Documento da política JSON .....	2011
Saiba mais .....	2012
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction .....	2012
A utilização desta política .....	2012
Detalhes da política .....	2012
Versão da política .....	2012
Documento da política JSON .....	2013
Saiba mais .....	2013



AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction .....	2013
A utilização desta política .....	2013
Detalhes da política .....	2014
Versão da política .....	2014
Documento da política JSON .....	2014
Saiba mais .....	2014
AWSIoTDeviceDefenderUpdateCACertMitigationAction .....	2015
A utilização desta política .....	2015
Detalhes da política .....	2015
Versão da política .....	2015
Documento da política JSON .....	2015
Saiba mais .....	2016
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction .....	2016
A utilização desta política .....	2016
Detalhes da política .....	2016
Versão da política .....	2017
Documento da política JSON .....	2017
Saiba mais .....	2017
AWSIoTDeviceTesterForFreeRTOSFullAccess .....	2017
A utilização desta política .....	2018
Detalhes da política .....	2018
Versão da política .....	2018
Documento da política JSON .....	2018
Saiba mais .....	2024
AWSIoTDeviceTesterForGreengrassFullAccess .....	2024
A utilização desta política .....	2025
Detalhes da política .....	2025
Versão da política .....	2025
Documento da política JSON .....	2025
Saiba mais .....	2028
AWSIoTEventsFullAccess .....	2028
A utilização desta política .....	2028
Detalhes da política .....	2028
Versão da política .....	2029
Documento da política JSON .....	2029
Saiba mais .....	2029

AWSIoTEventsReadOnlyAccess .....	2029
A utilização desta política .....	2030
Detalhes da política .....	2030
Versão da política .....	2030
Documento da política JSON .....	2030
Saiba mais .....	2030
AWSIoTFleetHubFederationAccess .....	2031
A utilização desta política .....	2031
Detalhes da política .....	2031
Versão da política .....	2031
Documento da política JSON .....	2031
Saiba mais .....	2033
AWSIoTFleetwiseServiceRolePolicy .....	2033
A utilização desta política .....	2033
Detalhes da política .....	2034
Versão da política .....	2034
Documento da política JSON .....	2034
Saiba mais .....	2035
AWSIoTFullAccess .....	2035
A utilização desta política .....	2035
Detalhes da política .....	2035
Versão da política .....	2035
Documento da política JSON .....	2035
Saiba mais .....	2036
AWSIoTLogging .....	2036
A utilização desta política .....	2036
Detalhes da política .....	2036
Versão da política .....	2036
Documento da política JSON .....	2037
Saiba mais .....	2037
AWSIoTOTAUpdate .....	2037
A utilização desta política .....	2038
Detalhes da política .....	2038
Versão da política .....	2038
Documento da política JSON .....	2038
Saiba mais .....	2038

AWSIoTRoboRunnerFullAccess .....	2039
A utilização desta política .....	2039
Detalhes da política .....	2039
Versão da política .....	2039
Documento da política JSON .....	2039
Saiba mais .....	2040
AWSIoTRoboRunnerReadOnly .....	2040
A utilização desta política .....	2040
Detalhes da política .....	2040
Versão da política .....	2041
Documento da política JSON .....	2041
Saiba mais .....	2041
AWSIoTRoboRunnerServiceRolePolicy .....	2042
A utilização desta política .....	2042
Detalhes da política .....	2042
Versão da política .....	2042
Documento da política JSON .....	2042
Saiba mais .....	2043
AWSIoTRuleActions .....	2043
A utilização desta política .....	2043
Detalhes da política .....	2043
Versão da política .....	2043
Documento da política JSON .....	2044
Saiba mais .....	2044
AWSIoTSiteWiseConsoleFullAccess .....	2044
A utilização desta política .....	2045
Detalhes da política .....	2045
Versão da política .....	2045
Documento da política JSON .....	2045
Saiba mais .....	2047
AWSIoTSiteWiseFullAccess .....	2047
A utilização desta política .....	2048
Detalhes da política .....	2048
Versão da política .....	2048
Documento da política JSON .....	2048
Saiba mais .....	2048

AWSIoTSiteWiseMonitorPortalAccess .....	2049
A utilização desta política .....	2049
Detalhes da política .....	2049
Versão da política .....	2049
Documento da política JSON .....	2049
Saiba mais .....	2050
AWSIoTSiteWiseMonitorServiceRolePolicy .....	2051
A utilização desta política .....	2051
Detalhes da política .....	2051
Versão da política .....	2051
Documento da política JSON .....	2051
Saiba mais .....	2052
AWSIoTSiteWiseReadOnlyAccess .....	2052
A utilização desta política .....	2053
Detalhes da política .....	2053
Versão da política .....	2053
Documento da política JSON .....	2053
Saiba mais .....	2054
AWSIoTThingsRegistration .....	2054
A utilização desta política .....	2054
Detalhes da política .....	2054
Versão da política .....	2054
Documento da política JSON .....	2054
Saiba mais .....	2056
AWSIoTTwinMakerServiceRolePolicy .....	2056
A utilização desta política .....	2056
Detalhes desta política .....	2056
Versão da política .....	2056
Documento da política JSON .....	2057
Saiba mais .....	2058
AWSIoTWirelessDataAccess .....	2058
A utilização desta política .....	2058
Detalhes da política .....	2058
Versão da política .....	2059
Documento da política JSON .....	2059
Saiba mais .....	2059

AWSIoTWirelessFullAccess .....	2060
A utilização desta política .....	2060
Detalhes da política .....	2060
Versão da política .....	2060
Documento da política JSON .....	2060
Saiba mais .....	2061
AWSIoTWirelessFullPublishAccess .....	2061
A utilização desta política .....	2061
Detalhes da política .....	2061
Versão da política .....	2061
Documento da política JSON .....	2061
Saiba mais .....	2062
AWSIoTWirelessGatewayCertManager .....	2062
A utilização desta política .....	2062
Detalhes da política .....	2062
Versão da política .....	2063
Documento da política JSON .....	2063
Saiba mais .....	2063
AWSIoTWirelessLogging .....	2063
A utilização desta política .....	2064
Detalhes da política .....	2064
Versão da política .....	2064
Documento da política JSON .....	2064
Saiba mais .....	2065
AWSIoTWirelessReadOnlyAccess .....	2065
A utilização desta política .....	2065
Detalhes da política .....	2065
Versão da política .....	2065
Documento da política JSON .....	2065
Saiba mais .....	2066
AWSIPAMServiceRolePolicy .....	2066
Utilização desta política .....	2066
Detalhes desta política .....	2066
Versão da política .....	2067
Documento da política JSON .....	2067
Saiba mais .....	2068

AWSIQContractServiceRolePolicy .....	2068
A utilização desta política .....	2068
Detalhes da política .....	2068
Versão da política .....	2068
Documento da política JSON .....	2069
Saiba mais .....	2069
AWSIQFullAccess .....	2069
A utilização desta política .....	2069
Detalhes da política .....	2069
Versão da política .....	2070
Documento da política JSON .....	2070
Saiba mais .....	2070
AWSIQPermissionServiceRolePolicy .....	2071
A utilização desta política .....	2071
Detalhes da política .....	2071
Versão da política .....	2071
Documento da política JSON .....	2071
Saiba mais .....	2072
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy .....	2072
Utilização desta política .....	2073
Detalhes desta política .....	2073
Versão da política .....	2073
Documento da política JSON .....	2073
Saiba mais .....	2074
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy .....	2074
A utilização desta política .....	2074
Detalhes da política .....	2074
Versão da política .....	2074
Documento da política JSON .....	2075
Saiba mais .....	2075
AWSKeyManagementServicePowerUser .....	2075
A utilização desta política .....	2075
Detalhes da política .....	2075
Versão da política .....	2076
Documento da política JSON .....	2076
Saiba mais .....	2076

AWSLakeFormationCrossAccountManager .....	2077
A utilização desta política .....	2077
Detalhes da política .....	2077
Versão da política .....	2077
Documento da política JSON .....	2077
Saiba mais .....	2079
AWSLakeFormationDataAdmin .....	2079
A utilização desta política .....	2080
Detalhes da política .....	2080
Versão da política .....	2080
Documento da política JSON .....	2080
Saiba mais .....	2081
AWSLambda_FullAccess .....	2082
A utilização desta política .....	2082
Detalhes da política .....	2082
Versão da política .....	2082
Documento da política JSON .....	2082
Saiba mais .....	2083
AWSLambda_ReadOnlyAccess .....	2084
A utilização desta política .....	2084
Detalhes da política .....	2084
Versão da política .....	2084
Documento da política JSON .....	2084
Saiba mais .....	2086
AWSLambdaBasicExecutionRole .....	2086
A utilização desta política .....	2086
Detalhes da política .....	2086
Versão da política .....	2086
Documento da política JSON .....	2086
Saiba mais .....	2087
AWSLambdaDynamoDBExecutionRole .....	2087
A utilização desta política .....	2087
Detalhes da política .....	2087
Versão da política .....	2088
Documento da política JSON .....	2088
Saiba mais .....	2088

AWSLambdaENIManagementAccess .....	2089
A utilização desta política .....	2089
Detalhes da política .....	2089
Versão da política .....	2089
Documento da política JSON .....	2089
Saiba mais .....	2090
AWSLambdaExecute .....	2090
A utilização desta política .....	2090
Detalhes da política .....	2090
Versão da política .....	2090
Documento da política JSON .....	2091
Saiba mais .....	2091
AWSLambdaFullAccess .....	2091
A utilização desta política .....	2092
Detalhes da política .....	2092
Versão da política .....	2092
Documento da política JSON .....	2092
Saiba mais .....	2094
AWSLambdaInvocation-DynamoDB .....	2094
A utilização desta política .....	2094
Detalhes da política .....	2094
Versão da política .....	2094
Documento da política JSON .....	2094
Saiba mais .....	2095
AWSLambdaKinesisExecutionRole .....	2095
A utilização desta política .....	2095
Detalhes da política .....	2096
Versão da política .....	2096
Documento da política JSON .....	2096
Saiba mais .....	2097
AWSLambdaMSKExecutionRole .....	2097
A utilização desta política .....	2097
Detalhes da política .....	2097
Versão da política .....	2097
Documento da política JSON .....	2097
Saiba mais .....	2098



AWSLambdaReplicator .....	2098
A utilização desta política .....	2098
Detalhes da política .....	2099
Versão da política .....	2099
Documento da política JSON .....	2099
Saiba mais .....	2100
AWSLambdaRole .....	2100
A utilização desta política .....	2100
Detalhes da política .....	2100
Versão da política .....	2101
Documento da política JSON .....	2101
Saiba mais .....	2101
AWSLambdaSQSQueueExecutionRole .....	2102
A utilização desta política .....	2102
Detalhes da política .....	2102
Versão da política .....	2102
Documento da política JSON .....	2102
Saiba mais .....	2103
AWSLambdaVPCLambdaAccessExecutionRole .....	2103
Utilização desta política .....	2103
Detalhes desta política .....	2103
Versão da política .....	2103
Documento da política JSON .....	2104
Saiba mais .....	2104
AWSLicenseManagerConsumptionPolicy .....	2104
A utilização desta política .....	2105
Detalhes da política .....	2105
Versão da política .....	2105
Documento da política JSON .....	2105
Saiba mais .....	2106
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy .....	2106
A utilização desta política .....	2106
Detalhes da política .....	2106
Versão da política .....	2106
Documento da política JSON .....	2107
Saiba mais .....	2107

AWSLicenseManagerMasterAccountRolePolicy .....	2108
A utilização desta política .....	2108
Detalhes da política .....	2108
Versão da política .....	2108
Documento da política JSON .....	2108
Saiba mais .....	2113
AWSLicenseManagerMemberAccountRolePolicy .....	2113
A utilização desta política .....	2113
Detalhes da política .....	2113
Versão da política .....	2114
Documento da política JSON .....	2114
Saiba mais .....	2115
AWSLicenseManagerServiceRolePolicy .....	2115
A utilização desta política .....	2115
Detalhes da política .....	2115
Versão da política .....	2116
Documento da política JSON .....	2116
Saiba mais .....	2119
AWSLicenseManagerUserSubscriptionsServiceRolePolicy .....	2119
A utilização desta política .....	2119
Detalhes da política .....	2120
Versão da política .....	2120
Documento da política JSON .....	2120
Saiba mais .....	2122
AWSM2ServicePolicy .....	2122
A utilização desta política .....	2122
Detalhes da política .....	2122
Versão da política .....	2123
Documento da política JSON .....	2123
Saiba mais .....	2124
AWSMangedServices_ContactsServiceRolePolicy .....	2124
A utilização desta política .....	2124
Detalhes da política .....	2124
Versão da política .....	2125
Documento da política JSON .....	2125
Saiba mais .....	2126

AWSMangedServices_DetectiveControlsConfig_ServiceRolePolicy .....	2126
A utilização desta política .....	2126
Detalhes da política .....	2126
Versão da política .....	2126
Documento da política JSON .....	2127
Saiba mais .....	2128
AWSMangedServices_EventsServiceRolePolicy .....	2128
A utilização desta política .....	2128
Detalhes da política .....	2128
Versão da política .....	2129
Documento da política JSON .....	2129
Saiba mais .....	2130
AWSMangedServicesDeploymentToolkitPolicy .....	2130
A utilização desta política .....	2130
Detalhes da política .....	2130
Versão da política .....	2130
Documento da política JSON .....	2130
Saiba mais .....	2132
AWSMarketplaceAmilngestion .....	2133
A utilização desta política .....	2133
Detalhes da política .....	2133
Versão da política .....	2133
Documento da política JSON .....	2133
Saiba mais .....	2134
AWSMarketplaceDeploymentServiceRolePolicy .....	2134
Utilização desta política .....	2134
Detalhes desta política .....	2134
Versão da política .....	2135
Documento da política JSON .....	2135
Saiba mais .....	2136
AWSMarketplaceFullAccess .....	2136
A utilização desta política .....	2137
Detalhes da política .....	2137
Versão da política .....	2137
Documento da política JSON .....	2137
Saiba mais .....	2140

---

AWSMarketplaceGetEntitlements .....	2140
A utilização desta política .....	2141
Detalhes da política .....	2141
Versão da política .....	2141
Documento da política JSON .....	2141
Saiba mais .....	2141
AWSMarketplaceImageBuildFullAccess .....	2142
A utilização desta política .....	2142
Detalhes da política .....	2142
Versão da política .....	2142
Documento da política JSON .....	2142
Saiba mais .....	2146
AWSMarketplaceLicenseManagementServiceRolePolicy .....	2146
A utilização desta política .....	2146
Detalhes da política .....	2146
Versão da política .....	2147
Documento da política JSON .....	2147
Saiba mais .....	2147
AWSMarketplaceManageSubscriptions .....	2148
A utilização desta política .....	2148
Detalhes da política .....	2148
Versão da política .....	2148
Documento da política JSON .....	2148
Saiba mais .....	2149
AWSMarketplaceMeteringFullAccess .....	2149
A utilização desta política .....	2149
Detalhes da política .....	2149
Versão da política .....	2150
Documento da política JSON .....	2150
Saiba mais .....	2150
AWSMarketplaceMeteringRegisterUsage .....	2151
A utilização desta política .....	2151
Detalhes da política .....	2151
Versão da política .....	2151
Documento da política JSON .....	2151
Saiba mais .....	2152

AWSMarketplaceProcurementSystemAdminFullAccess .....	2152
A utilização desta política .....	2152
Detalhes da política .....	2152
Versão da política .....	2152
Documento da política JSON .....	2153
Saiba mais .....	2153
AWSMarketplacePurchaseOrdersServiceRolePolicy .....	2153
A utilização desta política .....	2153
Detalhes da política .....	2154
Versão da política .....	2154
Documento da política JSON .....	2154
Saiba mais .....	2154
AWSMarketplaceRead-only .....	2155
A utilização desta política .....	2155
Detalhes da política .....	2155
Versão da política .....	2155
Documento da política JSON .....	2155
Saiba mais .....	2156
AWSMarketplaceResaleAuthorizationServiceRolePolicy .....	2157
Utilização desta política .....	2157
Detalhes desta política .....	2157
Versão da política .....	2157
Documento da política JSON .....	2157
Saiba mais .....	2160
AWSMarketplaceSellerFullAccess .....	2160
Utilização desta política .....	2160
Detalhes desta política .....	2160
Versão da política .....	2160
Documento da política JSON .....	2160
Saiba mais .....	2164
AWSMarketplaceSellerProductsFullAccess .....	2164
A utilização desta política .....	2164
Detalhes da política .....	2164
Versão da política .....	2165
Documento da política JSON .....	2165
Saiba mais .....	2167

---

AWSMarketplaceSellerProductsReadOnly .....	2167
A utilização desta política .....	2167
Detalhes da política .....	2167
Versão da política .....	2167
Documento da política JSON .....	2167
Saiba mais .....	2168
AWSMediaConnectServicePolicy .....	2168
A utilização desta política .....	2169
Detalhes da política .....	2169
Versão da política .....	2169
Documento da política JSON .....	2169
Saiba mais .....	2170
AWSMediaTailorServiceRolePolicy .....	2171
A utilização desta política .....	2171
Detalhes da política .....	2171
Versão da política .....	2171
Documento da política JSON .....	2171
Saiba mais .....	2172
AWSMigrationHubDiscoveryAccess .....	2172
A utilização desta política .....	2172
Detalhes da política .....	2172
Versão da política .....	2172
Documento da política JSON .....	2173
Saiba mais .....	2174
AWSMigrationHubDMSAccess .....	2174
A utilização desta política .....	2174
Detalhes da política .....	2174
Versão da política .....	2175
Documento da política JSON .....	2175
Saiba mais .....	2176
AWSMigrationHubFullAccess .....	2176
A utilização desta política .....	2176
Detalhes da política .....	2176
Versão da política .....	2176
Documento da política JSON .....	2177
Saiba mais .....	2178

AWSMigrationHubOrchestratorConsoleFullAccess .....	2178
Utilização desta política .....	2178
Detalhes desta política .....	2178
Versão da política .....	2179
Documento da política JSON .....	2179
Saiba mais .....	2182
AWSMigrationHubOrchestratorInstanceRolePolicy .....	2182
A utilização desta política .....	2182
Detalhes da política .....	2182
Versão da política .....	2183
Documento da política JSON .....	2183
Saiba mais .....	2183
AWSMigrationHubOrchestratorPlugin .....	2184
A utilização desta política .....	2184
Detalhes da política .....	2184
Versão da política .....	2184
Documento da política JSON .....	2184
Saiba mais .....	2186
AWSMigrationHubOrchestratorServiceRolePolicy .....	2186
Utilização desta política .....	2186
Detalhes desta política .....	2186
Versão da política .....	2186
Documento da política JSON .....	2187
Saiba mais .....	2190
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess .....	2190
A utilização desta política .....	2191
Detalhes da política .....	2191
Versão da política .....	2191
Documento da política JSON .....	2191
Saiba mais .....	2196
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy .....	2196
A utilização desta política .....	2197
Detalhes da política .....	2197
Versão da política .....	2197
Documento da política JSON .....	2197
Saiba mais .....	2198

AWSMigrationHubRefactorSpacesFullAccess .....	2199
A utilização desta política .....	2199
Detalhes da política .....	2199
Versão da política .....	2199
Documento da política JSON .....	2199
Saiba mais .....	2205
AWSMigrationHubRefactorSpacesServiceRolePolicy .....	2206
A utilização desta política .....	2206
Detalhes da política .....	2206
Versão da política .....	2206
Documento da política JSON .....	2206
Saiba mais .....	2210
AWSMigrationHubSMSAccess .....	2210
A utilização desta política .....	2210
Detalhes da política .....	2210
Versão da política .....	2211
Documento da política JSON .....	2211
Saiba mais .....	2212
AWSMigrationHubStrategyCollector .....	2212
Utilização desta política .....	2212
Detalhes desta política .....	2212
Versão da política .....	2212
Documento da política JSON .....	2213
Saiba mais .....	2215
AWSMigrationHubStrategyConsoleFullAccess .....	2215
A utilização desta política .....	2215
Detalhes da política .....	2215
Versão da política .....	2215
Documento da política JSON .....	2216
Saiba mais .....	2217
AWSMigrationHubStrategyServiceRolePolicy .....	2218
A utilização desta política .....	2218
Detalhes da política .....	2218
Versão da política .....	2218
Documento da política JSON .....	2218
Saiba mais .....	2219



AWSMobileHub_FullAccess .....	2219
A utilização desta política .....	2220
Detalhes da política .....	2220
Versão da política .....	2220
Documento da política JSON .....	2220
Saiba mais .....	2222
AWSMobileHub_ReadOnly .....	2222
A utilização desta política .....	2222
Detalhes da política .....	2222
Versão da política .....	2222
Documento da política JSON .....	2223
Saiba mais .....	2224
AWSMSKReplicatorExecutionRole .....	2224
Utilização desta política .....	2224
Detalhes desta política .....	2224
Versão da política .....	2224
Documento da política JSON .....	2225
Saiba mais .....	2226
AWSNetworkFirewallServiceRolePolicy .....	2226
A utilização desta política .....	2226
Detalhes da política .....	2226
Versão da política .....	2227
Documento da política JSON .....	2227
Saiba mais .....	2228
AWSNetworkManagerCloudWANServiceRolePolicy .....	2229
A utilização desta política .....	2229
Detalhes da política .....	2229
Versão da política .....	2229
Documento da política JSON .....	2229
Saiba mais .....	2230
AWSNetworkManagerFullAccess .....	2230
A utilização desta política .....	2230
Detalhes da política .....	2230
Versão da política .....	2230
Documento da política JSON .....	2230
Saiba mais .....	2231

AWSNetworkManagerReadOnlyAccess .....	2231
A utilização desta política .....	2231
Detalhes da política .....	2232
Versão da política .....	2232
Documento da política JSON .....	2232
Saiba mais .....	2232
AWSNetworkManagerServiceRolePolicy .....	2233
A utilização desta política .....	2233
Detalhes da política .....	2233
Versão da política .....	2233
Documento da política JSON .....	2233
Saiba mais .....	2234
AWSOpsWorks_FullAccess .....	2235
A utilização desta política .....	2235
Detalhes da política .....	2235
Versão da política .....	2235
Documento da política JSON .....	2235
Saiba mais .....	2236
AWSOpsWorksCloudWatchLogs .....	2236
A utilização desta política .....	2237
Detalhes da política .....	2237
Versão da política .....	2237
Documento da política JSON .....	2237
Saiba mais .....	2238
AWSOpsWorksCMInstanceProfileRole .....	2238
A utilização desta política .....	2238
Detalhes da política .....	2238
Versão da política .....	2238
Documento da política JSON .....	2238
Saiba mais .....	2239
AWSOpsWorksCMServiceRole .....	2240
A utilização desta política .....	2240
Detalhes da política .....	2240
Versão da política .....	2240
Documento da política JSON .....	2240
Saiba mais .....	2244

AWSOpsWorksInstanceRegistration .....	2245
A utilização desta política .....	2245
Detalhes da política .....	2245
Versão da política .....	2245
Documento da política JSON .....	2245
Saiba mais .....	2246
AWSOpsWorksRegisterCLI_EC2 .....	2246
A utilização desta política .....	2246
Detalhes da política .....	2246
Versão da política .....	2246
Documento da política JSON .....	2247
Saiba mais .....	2247
AWSOpsWorksRegisterCLI_OnPremises .....	2248
A utilização desta política .....	2248
Detalhes da política .....	2248
Versão da política .....	2248
Documento da política JSON .....	2248
Saiba mais .....	2250
AWSOrganizationsFullAccess .....	2250
Utilização desta política .....	2250
Detalhes desta política .....	2250
Versão da política .....	2250
Documento da política JSON .....	2251
Saiba mais .....	2252
AWSOrganizationsReadOnlyAccess .....	2252
Utilização desta política .....	2252
Detalhes desta política .....	2252
Versão da política .....	2252
Documento da política JSON .....	2252
Saiba mais .....	2253
AWSOrganizationsServiceTrustPolicy .....	2253
A utilização desta política .....	2253
Detalhes da política .....	2254
Versão da política .....	2254
Documento da política JSON .....	2254
Saiba mais .....	2255

AWSOutpostsAuthorizeServerPolicy .....	2255
A utilização desta política .....	2255
Detalhes da política .....	2255
Versão da política .....	2255
Documento da política JSON .....	2255
Saiba mais .....	2256
AWSOutpostsServiceRolePolicy .....	2256
A utilização desta política .....	2256
Detalhes da política .....	2256
Versão da política .....	2257
Documento da política JSON .....	2257
Saiba mais .....	2257
AWSPanoramaApplianceRolePolicy .....	2257
A utilização desta política .....	2258
Detalhes da política .....	2258
Versão da política .....	2258
Documento da política JSON .....	2258
Saiba mais .....	2259
AWSPanoramaApplianceServiceRolePolicy .....	2259
A utilização desta política .....	2259
Detalhes da política .....	2259
Versão da política .....	2259
Documento da política JSON .....	2260
Saiba mais .....	2261
AWSPanoramaFullAccess .....	2261
A utilização desta política .....	2261
Detalhes da política .....	2261
Versão da política .....	2262
Documento da política JSON .....	2262
Saiba mais .....	2264
AWSPanoramaGreengrassGroupRolePolicy .....	2265
A utilização desta política .....	2265
Detalhes da política .....	2265
Versão da política .....	2265
Documento da política JSON .....	2265
Saiba mais .....	2267

---

AWSPanoramaSageMakerRolePolicy .....	2267
A utilização desta política .....	2267
Detalhes da política .....	2267
Versão da política .....	2267
Documento da política JSON .....	2267
Saiba mais .....	2268
AWSPanoramaServiceLinkedRolePolicy .....	2268
A utilização desta política .....	2268
Detalhes da política .....	2268
Versão da política .....	2269
Documento da política JSON .....	2269
Saiba mais .....	2271
AWSPanoramaServiceRolePolicy .....	2272
A utilização desta política .....	2272
Detalhes da política .....	2272
Versão da política .....	2272
Documento da política JSON .....	2272
Saiba mais .....	2279
AWSPriceListServiceFullAccess .....	2280
A utilização desta política .....	2280
Detalhes da política .....	2280
Versão da política .....	2280
Documento da política JSON .....	2280
Saiba mais .....	2281
AWSPrivateCAAuditor .....	2281
A utilização desta política .....	2281
Detalhes da política .....	2281
Versão da política .....	2281
Documento da política JSON .....	2281
Saiba mais .....	2282
AWSPrivateCAFullAccess .....	2282
A utilização desta política .....	2283
Detalhes da política .....	2283
Versão da política .....	2283
Documento da política JSON .....	2283
Saiba mais .....	2283

AWSPriateCAPrivilegedUser .....	2284
A utilização desta política .....	2284
Detalhes da política .....	2284
Versão da política .....	2284
Documento da política JSON .....	2284
Saiba mais .....	2285
AWSPriateCAReadOnly .....	2286
A utilização desta política .....	2286
Detalhes da política .....	2286
Versão da política .....	2286
Documento da política JSON .....	2286
Saiba mais .....	2287
AWSPriateCAUser .....	2287
A utilização desta política .....	2287
Detalhes da política .....	2287
Versão da política .....	2288
Documento da política JSON .....	2288
Saiba mais .....	2289
AWSPriateMarketplaceAdminFullAccess .....	2289
Utilização desta política .....	2289
Detalhes desta política .....	2289
Versão da política .....	2290
Documento da política JSON .....	2290
Saiba mais .....	2291
AWSPriateMarketplaceRequests .....	2292
A utilização desta política .....	2292
Detalhes da política .....	2292
Versão da política .....	2292
Documento da política JSON .....	2292
Saiba mais .....	2293
AWSPriateNetworksServiceRolePolicy .....	2293
A utilização desta política .....	2293
Detalhes da política .....	2293
Versão da política .....	2293
Documento da política JSON .....	2294
Saiba mais .....	2294

AWSProtonCodeBuildProvisioningBasicAccess .....	2294
A utilização desta política .....	2294
Detalhes da política .....	2294
Versão da política .....	2295
Documento da política JSON .....	2295
Saiba mais .....	2295
AWSProtonCodeBuildProvisioningServiceRolePolicy .....	2296
A utilização desta política .....	2296
Detalhes da política .....	2296
Versão da política .....	2296
Documento da política JSON .....	2296
Saiba mais .....	2298
AWSProtonDeveloperAccess .....	2298
A utilização desta política .....	2298
Detalhes da política .....	2298
Versão da política .....	2298
Documento da política JSON .....	2298
Saiba mais .....	2300
AWSProtonFullAccess .....	2301
A utilização desta política .....	2301
Detalhes da política .....	2301
Versão da política .....	2301
Documento da política JSON .....	2301
Saiba mais .....	2303
AWSProtonReadOnlyAccess .....	2303
A utilização desta política .....	2303
Detalhes da política .....	2303
Versão da política .....	2303
Documento da política JSON .....	2304
Saiba mais .....	2305
AWSProtonServiceGitSyncServiceRolePolicy .....	2305
A utilização desta política .....	2305
Detalhes da política .....	2306
Versão da política .....	2306
Documento da política JSON .....	2306
Saiba mais .....	2307

AWSProtonSyncServiceRolePolicy .....	2307
A utilização desta política .....	2307
Detalhes da política .....	2307
Versão da política .....	2307
Documento da política JSON .....	2308
Saiba mais .....	2309
AWSPurchaseOrdersServiceRolePolicy .....	2309
A utilização desta política .....	2309
Detalhes da política .....	2309
Versão da política .....	2309
Documento da política JSON .....	2309
Saiba mais .....	2310
AWSQuicksightAthenaAccess .....	2311
A utilização desta política .....	2311
Detalhes da política .....	2311
Versão da política .....	2311
Documento da política JSON .....	2311
Saiba mais .....	2313
AWSQuickSightDescribeRDS .....	2314
A utilização desta política .....	2314
Detalhes da política .....	2314
Versão da política .....	2314
Documento da política JSON .....	2314
Saiba mais .....	2315
AWSQuickSightDescribeRedshift .....	2315
A utilização desta política .....	2315
Detalhes da política .....	2315
Versão da política .....	2315
Documento da política JSON .....	2315
Saiba mais .....	2316
AWSQuickSightElasticsearchPolicy .....	2316
A utilização desta política .....	2316
Detalhes da política .....	2316
Versão da política .....	2317
Documento da política JSON .....	2317
Saiba mais .....	2318



AWSQuickSightIoTAnalyticsAccess .....	2318
A utilização desta política .....	2318
Detalhes da política .....	2318
Versão da política .....	2318
Documento da política JSON .....	2319
Saiba mais .....	2319
AWSQuickSightListIAM .....	2319
A utilização desta política .....	2319
Detalhes da política .....	2320
Versão da política .....	2320
Documento da política JSON .....	2320
Saiba mais .....	2320
AWSQuickSightOpenSearchPolicy .....	2321
A utilização desta política .....	2321
Detalhes da política .....	2321
Versão da política .....	2321
Documento da política JSON .....	2321
Saiba mais .....	2322
AWSQuickSightSageMakerPolicy .....	2322
A utilização desta política .....	2323
Detalhes da política .....	2323
Versão da política .....	2323
Documento da política JSON .....	2323
Saiba mais .....	2324
AWSQuickSightTimestreamPolicy .....	2325
A utilização desta política .....	2325
Detalhes da política .....	2325
Versão da política .....	2325
Documento da política JSON .....	2325
Saiba mais .....	2326
AWSReachabilityAnalyzerServiceRolePolicy .....	2326
A utilização desta política .....	2326
Detalhes da política .....	2326
Versão da política .....	2327
Documento da política JSON .....	2327
Saiba mais .....	2329

AWSRefactoringToolkitFullAccess .....	2329
Utilização desta política .....	2329
Detalhes desta política .....	2330
Versão da política .....	2330
Documento da política JSON .....	2330
Saiba mais .....	2343
AWSRefactoringToolkitSidecarPolicy .....	2344
A utilização desta política .....	2344
Detalhes da política .....	2344
Versão da política .....	2344
Documento da política JSON .....	2344
Saiba mais .....	2345
AWSrePostPrivateCloudWatchAccess .....	2346
A utilização desta política .....	2346
Detalhes desta política .....	2346
Versão da política .....	2346
Documento da política JSON .....	2346
Saiba mais .....	2347
AWSRepostSpaceSupportOperationsPolicy .....	2347
Utilização desta política .....	2347
Detalhes desta política .....	2347
Versão da política .....	2348
Documento da política JSON .....	2348
Saiba mais .....	2348
AWSResilienceHubAssessmentExecutionPolicy .....	2349
A utilização desta política .....	2349
Detalhes da política .....	2349
Versão da política .....	2349
Documento da política JSON .....	2349
Saiba mais .....	2353
AWSResourceAccessManagerFullAccess .....	2353
A utilização desta política .....	2354
Detalhes da política .....	2354
Versão da política .....	2354
Documento da política JSON .....	2354
Saiba mais .....	2354

AWSResourceAccessManagerReadOnlyAccess .....	2355
A utilização desta política .....	2355
Detalhes da política .....	2355
Versão da política .....	2355
Documento da política JSON .....	2355
Saiba mais .....	2356
AWSResourceAccessManagerResourceShareParticipantAccess .....	2356
A utilização desta política .....	2356
Detalhes da política .....	2356
Versão da política .....	2356
Documento da política JSON .....	2357
Saiba mais .....	2357
AWSResourceAccessManagerServiceRolePolicy .....	2357
A utilização desta política .....	2358
Detalhes da política .....	2358
Versão da política .....	2358
Documento da política JSON .....	2358
Saiba mais .....	2359
AWSResourceExplorerFullAccess .....	2359
Utilização desta política .....	2359
Detalhes desta política .....	2359
Versão da política .....	2360
Documento da política JSON .....	2360
Saiba mais .....	2361
AWSResourceExplorerOrganizationsAccess .....	2361
Utilização desta política .....	2361
Detalhes desta política .....	2361
Versão da política .....	2361
Documento da política JSON .....	2362
Saiba mais .....	2363
AWSResourceExplorerReadOnlyAccess .....	2363
Utilização desta política .....	2364
Detalhes desta política .....	2364
Versão da política .....	2364
Documento da política JSON .....	2364
Saiba mais .....	2365

---

AWSResourceExplorerServiceRolePolicy .....	2365
A utilização desta política .....	2365
Detalhes desta política .....	2365
Versão da política .....	2365
Documento da política JSON .....	2366
Saiba mais .....	2375
AWSResourceGroupsReadOnlyAccess .....	2375
A utilização desta política .....	2375
Detalhes da política .....	2375
Versão da política .....	2375
Documento da política JSON .....	2376
Saiba mais .....	2377
AWSRoboMaker_FullAccess .....	2377
A utilização desta política .....	2377
Detalhes da política .....	2377
Versão da política .....	2378
Documento da política JSON .....	2378
Saiba mais .....	2379
AWSRoboMakerReadOnlyAccess .....	2379
A utilização desta política .....	2379
Detalhes da política .....	2380
Versão da política .....	2380
Documento da política JSON .....	2380
Saiba mais .....	2380
AWSRoboMakerServicePolicy .....	2381
A utilização desta política .....	2381
Detalhes da política .....	2381
Versão da política .....	2381
Documento da política JSON .....	2381
Saiba mais .....	2383
AWSRoboMakerServiceRolePolicy .....	2383
A utilização desta política .....	2383
Detalhes da política .....	2383
Versão da política .....	2383
Documento da política JSON .....	2384
Saiba mais .....	2385

AWSRolesAnywhereServicePolicy .....	2385
A utilização desta política .....	2385
Detalhes da política .....	2385
Versão da política .....	2386
Documento da política JSON .....	2386
Saiba mais .....	2386
AWSS3OnOutpostsServiceRolePolicy .....	2387
A utilização desta política .....	2387
Detalhes da política .....	2387
Versão da política .....	2387
Documento da política JSON .....	2387
Saiba mais .....	2390
AWSSavingsPlansFullAccess .....	2390
A utilização desta política .....	2390
Detalhes da política .....	2390
Versão da política .....	2391
Documento da política JSON .....	2391
Saiba mais .....	2391
AWSSavingsPlansReadOnlyAccess .....	2391
A utilização desta política .....	2391
Detalhes da política .....	2392
Versão da política .....	2392
Documento da política JSON .....	2392
Saiba mais .....	2392
AWSSecurityHubFullAccess .....	2393
Utilização desta política .....	2393
Detalhes desta política .....	2393
Versão da política .....	2393
Documento da política JSON .....	2393
Saiba mais .....	2394
AWSSecurityHubOrganizationsAccess .....	2394
Utilização desta política .....	2394
Detalhes desta política .....	2395
Versão da política .....	2395
Documento da política JSON .....	2395
Saiba mais .....	2396

AWSSecurityHubReadOnlyAccess .....	2396
Utilização desta política .....	2397
Detalhes desta política .....	2397
Versão da política .....	2397
Documento da política JSON .....	2397
Saiba mais .....	2398
AWSSecurityHubServiceRolePolicy .....	2398
Utilização desta política .....	2398
Detalhes desta política .....	2398
Versão da política .....	2398
Documento da política JSON .....	2398
Saiba mais .....	2400
AWSServiceCatalogAdminFullAccess .....	2401
A utilização desta política .....	2401
Detalhes da política .....	2401
Versão da política .....	2401
Documento da política JSON .....	2401
Saiba mais .....	2404
AWSServiceCatalogAdminReadOnlyAccess .....	2404
A utilização desta política .....	2404
Detalhes da política .....	2404
Versão da política .....	2405
Documento da política JSON .....	2405
Saiba mais .....	2406
AWSServiceCatalogAppRegistryFullAccess .....	2406
Utilização desta política .....	2406
Detalhes desta política .....	2407
Versão da política .....	2407
Documento da política JSON .....	2407
Saiba mais .....	2409
AWSServiceCatalogAppRegistryReadOnlyAccess .....	2409
A utilização desta política .....	2410
Detalhes da política .....	2410
Versão da política .....	2410
Documento da política JSON .....	2410
Saiba mais .....	2411

AWSServiceCatalogAppRegistryServiceRolePolicy .....	2411
A utilização desta política .....	2411
Detalhes da política .....	2411
Versão da política .....	2411
Documento da política JSON .....	2412
Saiba mais .....	2413
AWSServiceCatalogEndUserFullAccess .....	2413
A utilização desta política .....	2413
Detalhes da política .....	2413
Versão da política .....	2413
Documento da política JSON .....	2414
Saiba mais .....	2416
AWSServiceCatalogEndUserReadOnlyAccess .....	2416
A utilização desta política .....	2416
Detalhes da política .....	2416
Versão da política .....	2416
Documento da política JSON .....	2417
Saiba mais .....	2418
AWSServiceCatalogOrgsDataSyncServiceRolePolicy .....	2419
A utilização desta política .....	2419
Detalhes da política .....	2419
Versão da política .....	2419
Documento da política JSON .....	2419
Saiba mais .....	2420
AWSServiceCatalogSyncServiceRolePolicy .....	2420
A utilização desta política .....	2420
Detalhes da política .....	2420
Versão da política .....	2420
Documento da política JSON .....	2421
Saiba mais .....	2422
AWSServiceRoleForAmazonEKSNodegroup .....	2422
Utilização desta política .....	2422
Detalhes desta política .....	2422
Versão da política .....	2422
Documento da política JSON .....	2423
Saiba mais .....	2427

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICEPOLICY .....	2427
A utilização desta política .....	2427
Detalhes da política .....	2427
Versão da política .....	2427
Documento da política JSON .....	2427
Saiba mais .....	2428
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsSERVICEPOLICY .....	2428
A utilização desta política .....	2428
Detalhes da política .....	2428
Versão da política .....	2429
Documento da política JSON .....	2429
Saiba mais .....	2429
AWSServiceRoleForCodeGuru-Profiler .....	2429
A utilização desta política .....	2430
Detalhes da política .....	2430
Versão da política .....	2430
Documento da política JSON .....	2430
Saiba mais .....	2431
AWSServiceRoleForCodeWhispererPolicy .....	2431
Utilização desta política .....	2431
Detalhes desta política .....	2431
Versão da política .....	2431
Documento da política JSON .....	2432
Saiba mais .....	2433
AWSServiceRoleForEC2ScheduledInstances .....	2433
A utilização desta política .....	2434
Detalhes da política .....	2434
Versão da política .....	2434
Documento da política JSON .....	2434
Saiba mais .....	2435
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy .....	2435
A utilização desta política .....	2435
Detalhes da política .....	2435
Versão da política .....	2436
Documento da política JSON .....	2436
Saiba mais .....	2436



AWSServiceRoleForImageBuilder .....	2436
A utilização desta política .....	2437
Detalhes da política .....	2437
Versão da política .....	2437
Documento da política JSON .....	2437
Saiba mais .....	2447
AWSServiceRoleForIoTSiteWise .....	2447
Utilização desta política .....	2447
Detalhes desta política .....	2447
Versão da política .....	2447
Documento da política JSON .....	2448
Saiba mais .....	2449
AWSServiceRoleForLogDeliveryPolicy .....	2449
A utilização desta política .....	2449
Detalhes da política .....	2449
Versão da política .....	2450
Documento da política JSON .....	2450
Saiba mais .....	2450
AWSServiceRoleForMonitronPolicy .....	2451
A utilização desta política .....	2451
Detalhes da política .....	2451
Versão da política .....	2451
Documento da política JSON .....	2451
Saiba mais .....	2452
AWSServiceRoleForNeptuneGraphPolicy .....	2452
A utilização desta política .....	2452
Detalhes desta política .....	2452
Versão da política .....	2452
Documento da política JSON .....	2453
Saiba mais .....	2454
AWSServiceRoleForPrivateMarketplaceAdminPolicy .....	2454
Utilização desta política .....	2454
Detalhes desta política .....	2454
Versão da política .....	2455
Documento da política JSON .....	2455
Saiba mais .....	2457

AWSServiceRoleForSMS .....	2457
A utilização desta política .....	2457
Detalhes da política .....	2457
Versão da política .....	2457
Documento da política JSON .....	2457
Saiba mais .....	2464
AWSServiceRolePolicyForBackupReports .....	2464
A utilização desta política .....	2464
Detalhes da política .....	2464
Versão da política .....	2465
Documento da política JSON .....	2465
Saiba mais .....	2466
AWSServiceRolePolicyForBackupRestoreTesting .....	2466
Utilização desta política .....	2466
Detalhes desta política .....	2467
Versão da política .....	2467
Documento da política JSON .....	2467
Saiba mais .....	2470
AWSShieldDRTAcessPolicy .....	2470
A utilização desta política .....	2470
Detalhes da política .....	2470
Versão da política .....	2470
Documento da política JSON .....	2471
Saiba mais .....	2472
AWSShieldServiceRolePolicy .....	2472
A utilização desta política .....	2472
Detalhes da política .....	2472
Versão da política .....	2472
Documento da política JSON .....	2472
Saiba mais .....	2473
AWSSSMForSAPServiceLinkedRolePolicy .....	2473
Utilização desta política .....	2473
Detalhes desta política .....	2473
Versão da política .....	2474
Documento da política JSON .....	2474
Saiba mais .....	2480

AWSSSMOpsInsightsServiceRolePolicy .....	2480
A utilização desta política .....	2480
Detalhes da política .....	2480
Versão da política .....	2481
Documento da política JSON .....	2481
Saiba mais .....	2482
AWSSSODirectoryAdministrator .....	2482
A utilização desta política .....	2482
Detalhes da política .....	2482
Versão da política .....	2482
Documento da política JSON .....	2482
Saiba mais .....	2483
AWSSSODirectoryReadOnly .....	2483
A utilização desta política .....	2483
Detalhes da política .....	2483
Versão da política .....	2484
Documento da política JSON .....	2484
Saiba mais .....	2484
AWSSSOMasterAccountAdministrator .....	2485
A utilização desta política .....	2485
Detalhes da política .....	2485
Versão da política .....	2485
Documento da política JSON .....	2485
Saiba mais .....	2487
AWSSSOMemberAccountAdministrator .....	2487
A utilização desta política .....	2487
Detalhes da política .....	2487
Versão da política .....	2488
Documento da política JSON .....	2488
Saiba mais .....	2489
AWSSSOReadOnly .....	2489
A utilização desta política .....	2489
Detalhes da política .....	2489
Versão da política .....	2490
Documento da política JSON .....	2490
Saiba mais .....	2491

AWSSSOServiceRolePolicy .....	2491
A utilização desta política .....	2491
Detalhes da política .....	2491
Versão da política .....	2491
Documento da política JSON .....	2492
Saiba mais .....	2495
AWSSStepFunctionsConsoleFullAccess .....	2495
A utilização desta política .....	2495
Detalhes da política .....	2496
Versão da política .....	2496
Documento da política JSON .....	2496
Saiba mais .....	2497
AWSSStepFunctionsFullAccess .....	2497
A utilização desta política .....	2497
Detalhes da política .....	2497
Versão da política .....	2497
Documento da política JSON .....	2498
Saiba mais .....	2498
AWSSStepFunctionsReadOnlyAccess .....	2498
A utilização desta política .....	2498
Detalhes da política .....	2498
Versão da política .....	2499
Documento da política JSON .....	2499
Saiba mais .....	2499
AWSSStorageGatewayFullAccess .....	2500
A utilização desta política .....	2500
Detalhes da política .....	2500
Versão da política .....	2500
Documento da política JSON .....	2500
Saiba mais .....	2501
AWSSStorageGatewayReadOnlyAccess .....	2501
A utilização desta política .....	2501
Detalhes da política .....	2501
Versão da política .....	2502
Documento da política JSON .....	2502
Saiba mais .....	2502

---

AWSSStorageGatewayServiceRolePolicy .....	2503
A utilização desta política .....	2503
Detalhes da política .....	2503
Versão da política .....	2503
Documento da política JSON .....	2503
Saiba mais .....	2504
AWSSupplyChainFederationAdminAccess .....	2504
Utilização desta política .....	2504
Detalhes desta política .....	2504
Versão da política .....	2505
Documento da política JSON .....	2505
Saiba mais .....	2510
AWSSupportAccess .....	2510
A utilização desta política .....	2510
Detalhes da política .....	2510
Versão da política .....	2511
Documento da política JSON .....	2511
Saiba mais .....	2511
AWSSupportAppFullAccess .....	2512
A utilização desta política .....	2512
Detalhes da política .....	2512
Versão da política .....	2512
Documento da política JSON .....	2512
Saiba mais .....	2513
AWSSupportAppReadOnlyAccess .....	2513
A utilização desta política .....	2513
Detalhes da política .....	2514
Versão da política .....	2514
Documento da política JSON .....	2514
Saiba mais .....	2514
AWSSupportPlansFullAccess .....	2515
A utilização desta política .....	2515
Detalhes da política .....	2515
Versão da política .....	2515
Documento da política JSON .....	2515
Saiba mais .....	2516

AWSSupportPlansReadOnlyAccess .....	2516
A utilização desta política .....	2516
Detalhes da política .....	2516
Versão da política .....	2516
Documento da política JSON .....	2516
Saiba mais .....	2517
AWSSupportServiceRolePolicy .....	2517
Utilização desta política .....	2517
Detalhes desta política .....	2517
Versão da política .....	2518
Documento da política JSON .....	2518
Saiba mais .....	2591
AWSSystemsManagerAccountDiscoveryServicePolicy .....	2592
A utilização desta política .....	2592
Detalhes da política .....	2592
Versão da política .....	2592
Documento da política JSON .....	2592
Saiba mais .....	2593
AWSSystemsManagerChangeManagementServicePolicy .....	2593
A utilização desta política .....	2593
Detalhes da política .....	2593
Versão da política .....	2594
Documento da política JSON .....	2594
Saiba mais .....	2595
AWSSystemsManagerForSAPFullAccess .....	2596
A utilização desta política .....	2596
Detalhes da política .....	2596
Versão da política .....	2596
Documento da política JSON .....	2596
Saiba mais .....	2597
AWSSystemsManagerForSAPReadOnlyAccess .....	2597
A utilização desta política .....	2597
Detalhes da política .....	2597
Versão da política .....	2598
Documento da política JSON .....	2598
Saiba mais .....	2598

AWSSystemsManagerOpsDataSyncServiceRolePolicy .....	2598
A utilização desta política .....	2599
Detalhes da política .....	2599
Versão da política .....	2599
Documento da política JSON .....	2599
Saiba mais .....	2603
AWSThinkboxAssetServerPolicy .....	2603
A utilização desta política .....	2603
Detalhes da política .....	2603
Versão da política .....	2603
Documento da política JSON .....	2603
Saiba mais .....	2604
AWSThinkboxAWSPortalAdminPolicy .....	2604
Utilização desta política .....	2605
Detalhes desta política .....	2605
Versão da política .....	2605
Documento da política JSON .....	2605
Saiba mais .....	2615
AWSThinkboxAWSPortalGatewayPolicy .....	2615
A utilização desta política .....	2615
Detalhes da política .....	2615
Versão da política .....	2616
Documento da política JSON .....	2616
Saiba mais .....	2617
AWSThinkboxAWSPortalWorkerPolicy .....	2618
A utilização desta política .....	2618
Detalhes da política .....	2618
Versão da política .....	2618
Documento da política JSON .....	2618
Saiba mais .....	2620
AWSThinkboxDeadlineResourceTrackerAccessPolicy .....	2621
A utilização desta política .....	2621
Detalhes da política .....	2621
Versão da política .....	2621
Documento da política JSON .....	2621
Saiba mais .....	2624

---

AWSThinkboxDeadlineResourceTrackerAdminPolicy .....	2624
A utilização desta política .....	2624
Detalhes da política .....	2624
Versão da política .....	2625
Documento da política JSON .....	2625
Saiba mais .....	2630
AWSThinkboxDeadlineSpotEventPluginAdminPolicy .....	2631
A utilização desta política .....	2631
Detalhes da política .....	2631
Versão da política .....	2631
Documento da política JSON .....	2631
Saiba mais .....	2634
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy .....	2634
A utilização desta política .....	2634
Detalhes da política .....	2635
Versão da política .....	2635
Documento da política JSON .....	2635
Saiba mais .....	2636
AWSTransferConsoleFullAccess .....	2637
A utilização desta política .....	2637
Detalhes da política .....	2637
Versão da política .....	2637
Documento da política JSON .....	2637
Saiba mais .....	2638
AWSTransferFullAccess .....	2638
A utilização desta política .....	2638
Detalhes da política .....	2639
Versão da política .....	2639
Documento da política JSON .....	2639
Saiba mais .....	2640
AWSTransferLoggingAccess .....	2640
A utilização desta política .....	2640
Detalhes da política .....	2640
Versão da política .....	2640
Documento da política JSON .....	2641
Saiba mais .....	2641



AWSTransferReadOnlyAccess .....	2641
A utilização desta política .....	2641
Detalhes da política .....	2642
Versão da política .....	2642
Documento da política JSON .....	2642
Saiba mais .....	2642
AWSTrustedAdvisorPriorityFullAccess .....	2643
A utilização desta política .....	2643
Detalhes da política .....	2643
Versão da política .....	2643
Documento da política JSON .....	2643
Saiba mais .....	2645
AWSTrustedAdvisorPriorityReadOnlyAccess .....	2645
A utilização desta política .....	2646
Detalhes da política .....	2646
Versão da política .....	2646
Documento da política JSON .....	2646
Saiba mais .....	2647
AWSTrustedAdvisorReportingServiceRolePolicy .....	2647
A utilização desta política .....	2647
Detalhes da política .....	2648
Versão da política .....	2648
Documento da política JSON .....	2648
Saiba mais .....	2649
AWSTrustedAdvisorServiceRolePolicy .....	2649
Utilização desta política .....	2649
Detalhes desta política .....	2649
Versão da política .....	2649
Documento da política JSON .....	2649
Saiba mais .....	2652
AWSUserNotificationsServiceLinkedRolePolicy .....	2652
A utilização desta política .....	2652
Detalhes da política .....	2652
Versão da política .....	2653
Documento da política JSON .....	2653
Saiba mais .....	2654

AWSVendorInsightsAssessorFullAccess .....	2654
A utilização desta política .....	2654
Detalhes da política .....	2654
Versão da política .....	2654
Documento da política JSON .....	2655
Saiba mais .....	2656
AWSVendorInsightsAssessorReadOnly .....	2656
A utilização desta política .....	2656
Detalhes da política .....	2656
Versão da política .....	2656
Documento da política JSON .....	2657
Saiba mais .....	2657
AWSVendorInsightsVendorFullAccess .....	2657
A utilização desta política .....	2658
Detalhes da política .....	2658
Versão da política .....	2658
Documento da política JSON .....	2658
Saiba mais .....	2660
AWSVendorInsightsVendorReadOnly .....	2660
A utilização desta política .....	2660
Detalhes da política .....	2660
Versão da política .....	2660
Documento da política JSON .....	2661
Saiba mais .....	2662
AWSVpcLatticeServiceRolePolicy .....	2662
A utilização desta política .....	2662
Detalhes da política .....	2662
Versão da política .....	2662
Documento da política JSON .....	2663
Saiba mais .....	2663
AWSVPCS2SVpnServiceRolePolicy .....	2663
A utilização desta política .....	2663
Detalhes da política .....	2663
Versão da política .....	2664
Documento da política JSON .....	2664
Saiba mais .....	2664

AWSVPCTransitGatewayServiceRolePolicy .....	2665
A utilização desta política .....	2665
Detalhes da política .....	2665
Versão da política .....	2665
Documento da política JSON .....	2665
Saiba mais .....	2666
AWSVPCVerifiedAccessServiceRolePolicy .....	2666
Utilização desta política .....	2666
Detalhes desta política .....	2666
Versão da política .....	2666
Documento da política JSON .....	2667
Saiba mais .....	2668
AWSWAFConsoleFullAccess .....	2668
A utilização desta política .....	2669
Detalhes da política .....	2669
Versão da política .....	2669
Documento da política JSON .....	2669
Saiba mais .....	2671
AWSWAFConsoleReadOnlyAccess .....	2671
A utilização desta política .....	2672
Detalhes da política .....	2672
Versão da política .....	2672
Documento da política JSON .....	2672
Saiba mais .....	2673
AWSWAFFullAccess .....	2673
A utilização desta política .....	2673
Detalhes da política .....	2673
Versão da política .....	2674
Documento da política JSON .....	2674
Saiba mais .....	2676
AWSWAFReadOnlyAccess .....	2676
A utilização desta política .....	2676
Detalhes da política .....	2676
Versão da política .....	2676
Documento da política JSON .....	2676
Saiba mais .....	2677

AWSWellArchitectedDiscoveryServiceRolePolicy .....	2677
A utilização desta política .....	2678
Detalhes da política .....	2678
Versão da política .....	2678
Documento da política JSON .....	2678
Saiba mais .....	2680
AWSWellArchitectedOrganizationsServiceRolePolicy .....	2680
A utilização desta política .....	2680
Detalhes da política .....	2680
Versão da política .....	2680
Documento da política JSON .....	2680
Saiba mais .....	2681
AWSWickrFullAccess .....	2681
A utilização desta política .....	2681
Detalhes da política .....	2681
Versão da política .....	2682
Documento da política JSON .....	2682
Saiba mais .....	2682
AWSXrayCrossAccountSharingConfiguration .....	2682
A utilização desta política .....	2683
Detalhes da política .....	2683
Versão da política .....	2683
Documento da política JSON .....	2683
Saiba mais .....	2684
AWSXRayDaemonWriteAccess .....	2684
Utilização desta política .....	2684
Detalhes desta política .....	2684
Versão da política .....	2685
Documento da política JSON .....	2685
Saiba mais .....	2685
AWSXrayFullAccess .....	2686
A utilização desta política .....	2686
Detalhes da política .....	2686
Versão da política .....	2686
Documento da política JSON .....	2686
Saiba mais .....	2687

AWSXrayReadOnlyAccess .....	2687
Utilização desta política .....	2687
Detalhes desta política .....	2687
Versão da política .....	2687
Documento da política JSON .....	2688
Saiba mais .....	2688
AWSXrayWriteOnlyAccess .....	2689
A utilização desta política .....	2689
Detalhes da política .....	2689
Versão da política .....	2689
Documento da política JSON .....	2689
Saiba mais .....	2690
AWSZonalAutoshiftPracticeRunSLRPolicy .....	2690
A utilização desta política .....	2690
Detalhes desta política .....	2690
Versão da política .....	2690
Documento da política JSON .....	2691
Saiba mais .....	2691
BatchServiceRolePolicy .....	2692
Utilização desta política .....	2692
Detalhes desta política .....	2692
Versão da política .....	2692
Documento da política JSON .....	2692
Saiba mais .....	2698
Billing .....	2699
Utilização desta política .....	2699
Detalhes desta política .....	2699
Versão da política .....	2699
Documento da política JSON .....	2699
Saiba mais .....	2702
CertificateManagerServiceRolePolicy .....	2702
A utilização desta política .....	2702
Detalhes da política .....	2702
Versão da política .....	2703
Documento da política JSON .....	2703
Saiba mais .....	2703

ClientVPNServiceConnectionsRolePolicy .....	2703
A utilização desta política .....	2703
Detalhes da política .....	2704
Versão da política .....	2704
Documento da política JSON .....	2704
Saiba mais .....	2704
ClientVPNServiceRolePolicy .....	2705
A utilização desta política .....	2705
Detalhes da política .....	2705
Versão da política .....	2705
Documento da política JSON .....	2705
Saiba mais .....	2706
CloudFormationStackSetsOrgAdminServiceRolePolicy .....	2706
A utilização desta política .....	2706
Detalhes da política .....	2706
Versão da política .....	2707
Documento da política JSON .....	2707
Saiba mais .....	2707
CloudFormationStackSetsOrgMemberServiceRolePolicy .....	2708
A utilização desta política .....	2708
Detalhes da política .....	2708
Versão da política .....	2708
Documento da política JSON .....	2708
Saiba mais .....	2709
CloudFrontFullAccess .....	2709
Utilização desta política .....	2709
Detalhes desta política .....	2709
Versão da política .....	2710
Documento da política JSON .....	2710
Saiba mais .....	2711
CloudFrontReadOnlyAccess .....	2711
Utilização desta política .....	2711
Detalhes desta política .....	2712
Versão da política .....	2712
Documento da política JSON .....	2712
Saiba mais .....	2713

CloudHSMSERVICERolePolicy .....	2713
A utilização desta política .....	2713
Detalhes da política .....	2713
Versão da política .....	2713
Documento da política JSON .....	2714
Saiba mais .....	2714
CloudSearchFullAccess .....	2714
A utilização desta política .....	2714
Detalhes da política .....	2714
Versão da política .....	2715
Documento da política JSON .....	2715
Saiba mais .....	2715
CloudSearchReadOnlyAccess .....	2715
A utilização desta política .....	2716
Detalhes da política .....	2716
Versão da política .....	2716
Documento da política JSON .....	2716
Saiba mais .....	2716
CloudTrailServiceRolePolicy .....	2717
A utilização desta política .....	2717
Detalhes desta política .....	2717
Versão da política .....	2717
Documento da política JSON .....	2717
Saiba mais .....	2719
CloudWatch-CrossAccountAccess .....	2719
A utilização desta política .....	2719
Detalhes da política .....	2719
Versão da política .....	2720
Documento da política JSON .....	2720
Saiba mais .....	2720
CloudWatchActionsEC2Access .....	2720
A utilização desta política .....	2721
Detalhes da política .....	2721
Versão da política .....	2721
Documento da política JSON .....	2721
Saiba mais .....	2722

CloudWatchAgentAdminPolicy .....	2722
Utilização desta política .....	2722
Detalhes desta política .....	2722
Versão da política .....	2722
Documento da política JSON .....	2722
Saiba mais .....	2723
CloudWatchAgentServerPolicy .....	2724
Utilização desta política .....	2724
Detalhes desta política .....	2724
Versão da política .....	2724
Documento da política JSON .....	2724
Saiba mais .....	2725
CloudWatchApplicationInsightsFullAccess .....	2725
A utilização desta política .....	2725
Detalhes da política .....	2726
Versão da política .....	2726
Documento da política JSON .....	2726
Saiba mais .....	2727
CloudWatchApplicationInsightsReadOnlyAccess .....	2728
A utilização desta política .....	2728
Detalhes da política .....	2728
Versão da política .....	2728
Documento da política JSON .....	2728
Saiba mais .....	2729
CloudwatchApplicationInsightsServiceLinkedRolePolicy .....	2729
A utilização desta política .....	2729
Detalhes da política .....	2729
Versão da política .....	2729
Documento da política JSON .....	2730
Saiba mais .....	2739
CloudWatchApplicationSignalsServiceRolePolicy .....	2739
Utilização desta política .....	2740
Detalhes desta política .....	2740
Versão da política .....	2740
Documento da política JSON .....	2740
Saiba mais .....	2742



CloudWatchAutomaticDashboardsAccess .....	2742
A utilização desta política .....	2742
Detalhes da política .....	2742
Versão da política .....	2742
Documento da política JSON .....	2743
Saiba mais .....	2744
CloudWatchCrossAccountSharingConfiguration .....	2744
A utilização desta política .....	2744
Detalhes da política .....	2744
Versão da política .....	2745
Documento da política JSON .....	2745
Saiba mais .....	2746
CloudWatchEventsBuiltInTargetExecutionAccess .....	2746
A utilização desta política .....	2746
Detalhes da política .....	2746
Versão da política .....	2746
Documento da política JSON .....	2747
Saiba mais .....	2747
CloudWatchEventsFullAccess .....	2747
A utilização desta política .....	2748
Detalhes da política .....	2748
Versão da política .....	2748
Documento da política JSON .....	2748
Saiba mais .....	2750
CloudWatchEventsInvocationAccess .....	2750
A utilização desta política .....	2750
Detalhes da política .....	2750
Versão da política .....	2751
Documento da política JSON .....	2751
Saiba mais .....	2751
CloudWatchEventsReadOnlyAccess .....	2752
A utilização desta política .....	2752
Detalhes da política .....	2752
Versão da política .....	2752
Documento da política JSON .....	2752
Saiba mais .....	2753

CloudWatchEventsServiceRolePolicy .....	2754
A utilização desta política .....	2754
Detalhes da política .....	2754
Versão da política .....	2754
Documento da política JSON .....	2754
Saiba mais .....	2755
CloudWatchFullAccess .....	2755
A utilização desta política .....	2755
Detalhes da política .....	2755
Versão da política .....	2756
Documento da política JSON .....	2756
Saiba mais .....	2757
CloudWatchFullAccessV2 .....	2757
Utilização desta política .....	2757
Detalhes desta política .....	2757
Versão da política .....	2757
Documento da política JSON .....	2758
Saiba mais .....	2759
CloudWatchInternetMonitorServiceRolePolicy .....	2759
A utilização desta política .....	2760
Detalhes da política .....	2760
Versão da política .....	2760
Documento da política JSON .....	2760
Saiba mais .....	2761
CloudWatchLambdaInsightsExecutionRolePolicy .....	2761
A utilização desta política .....	2761
Detalhes da política .....	2762
Versão da política .....	2762
Documento da política JSON .....	2762
Saiba mais .....	2762
CloudWatchLogsCrossAccountSharingConfiguration .....	2763
A utilização desta política .....	2763
Detalhes da política .....	2763
Versão da política .....	2763
Documento da política JSON .....	2763
Saiba mais .....	2764

CloudWatchLogsFullAccess .....	2765
Utilização desta política .....	2765
Detalhes desta política .....	2765
Versão da política .....	2765
Documento da política JSON .....	2765
Saiba mais .....	2766
CloudWatchLogsReadOnlyAccess .....	2766
Utilização desta política .....	2766
Detalhes desta política .....	2766
Versão da política .....	2766
Documento da política JSON .....	2767
Saiba mais .....	2767
CloudWatchNetworkMonitorServiceRolePolicy .....	2767
A utilização desta política .....	2768
Detalhes desta política .....	2768
Versão da política .....	2768
Documento da política JSON .....	2768
Saiba mais .....	2769
CloudWatchReadOnlyAccess .....	2770
Utilização desta política .....	2770
Detalhes desta política .....	2770
Versão da política .....	2770
Documento da política JSON .....	2770
Saiba mais .....	2771
CloudWatchSyntheticsFullAccess .....	2772
A utilização desta política .....	2772
Detalhes da política .....	2772
Versão da política .....	2772
Documento da política JSON .....	2772
Saiba mais .....	2777
CloudWatchSyntheticsReadOnlyAccess .....	2777
A utilização desta política .....	2777
Detalhes da política .....	2777
Versão da política .....	2778
Documento da política JSON .....	2778
Saiba mais .....	2778

---

ComprehendDataAccessRolePolicy .....	2778
A utilização desta política .....	2779
Detalhes da política .....	2779
Versão da política .....	2779
Documento da política JSON .....	2779
Saiba mais .....	2780
ComprehendFullAccess .....	2780
A utilização desta política .....	2780
Detalhes da política .....	2780
Versão da política .....	2780
Documento da política JSON .....	2780
Saiba mais .....	2781
ComprehendMedicalFullAccess .....	2781
A utilização desta política .....	2781
Detalhes da política .....	2781
Versão da política .....	2782
Documento da política JSON .....	2782
Saiba mais .....	2782
ComprehendReadOnly .....	2782
A utilização desta política .....	2782
Detalhes da política .....	2783
Versão da política .....	2783
Documento da política JSON .....	2783
Saiba mais .....	2784
ComputeOptimizerReadOnlyAccess .....	2784
A utilização desta política .....	2785
Detalhes da política .....	2785
Versão da política .....	2785
Documento da política JSON .....	2785
Saiba mais .....	2786
ComputeOptimizerServiceRolePolicy .....	2786
A utilização desta política .....	2786
Detalhes da política .....	2786
Versão da política .....	2787
Documento da política JSON .....	2787
Saiba mais .....	2788

ConfigConformsServiceRolePolicy .....	2788
A utilização desta política .....	2789
Detalhes da política .....	2789
Versão da política .....	2789
Documento da política JSON .....	2789
Saiba mais .....	2792
CostOptimizationHubAdminAccess .....	2792
Utilização desta política .....	2792
Detalhes desta política .....	2792
Versão da política .....	2792
Documento da política JSON .....	2793
Saiba mais .....	2794
CostOptimizationHubReadOnlyAccess .....	2794
Utilização desta política .....	2794
Detalhes desta política .....	2794
Versão da política .....	2795
Documento da política JSON .....	2795
Saiba mais .....	2795
CostOptimizationHubServiceRolePolicy .....	2796
A utilização desta política .....	2796
Detalhes desta política .....	2796
Versão da política .....	2796
Documento da política JSON .....	2796
Saiba mais .....	2797
CustomerProfilesServiceLinkedRolePolicy .....	2797
A utilização desta política .....	2797
Detalhes da política .....	2797
Versão da política .....	2798
Documento da política JSON .....	2798
Saiba mais .....	2799
DatabaseAdministrator .....	2799
A utilização desta política .....	2799
Detalhes da política .....	2799
Versão da política .....	2799
Documento da política JSON .....	2799
Saiba mais .....	2802

DataScientist .....	2802
A utilização desta política .....	2802
Detalhes da política .....	2802
Versão da política .....	2802
Documento da política JSON .....	2803
Saiba mais .....	2806
DAXServiceRolePolicy .....	2807
A utilização desta política .....	2807
Detalhes da política .....	2807
Versão da política .....	2807
Documento da política JSON .....	2807
Saiba mais .....	2808
DynamoDBCloudWatchContributorInsightsServiceRolePolicy .....	2808
A utilização desta política .....	2808
Detalhes da política .....	2808
Versão da política .....	2809
Documento da política JSON .....	2809
Saiba mais .....	2809
DynamoDBKinesisReplicationServiceRolePolicy .....	2810
A utilização desta política .....	2810
Detalhes da política .....	2810
Versão da política .....	2810
Documento da política JSON .....	2810
Saiba mais .....	2811
DynamoDBReplicationServiceRolePolicy .....	2811
Utilização desta política .....	2811
Detalhes desta política .....	2811
Versão da política .....	2812
Documento da política JSON .....	2812
Saiba mais .....	2813
EC2FastLaunchServiceRolePolicy .....	2813
A utilização desta política .....	2813
Detalhes da política .....	2813
Versão da política .....	2814
Documento da política JSON .....	2814
Saiba mais .....	2818

EC2FleetTimeShiftableServiceRolePolicy .....	2818
A utilização desta política .....	2818
Detalhes da política .....	2818
Versão da política .....	2818
Documento da política JSON .....	2818
Saiba mais .....	2820
Ec2ImageBuilderCrossAccountDistributionAccess .....	2820
A utilização desta política .....	2820
Detalhes da política .....	2820
Versão da política .....	2820
Documento da política JSON .....	2821
Saiba mais .....	2821
EC2ImageBuilderLifecycleExecutionPolicy .....	2821
Utilização desta política .....	2822
Detalhes desta política .....	2822
Versão da política .....	2822
Documento da política JSON .....	2822
Saiba mais .....	2824
EC2InstanceConnect .....	2824
A utilização desta política .....	2824
Detalhes da política .....	2825
Versão da política .....	2825
Documento da política JSON .....	2825
Saiba mais .....	2825
Ec2InstanceConnectEndpoint .....	2826
A utilização desta política .....	2826
Detalhes da política .....	2826
Versão da política .....	2826
Documento da política JSON .....	2826
Saiba mais .....	2828
EC2InstanceProfileForImageBuilder .....	2828
A utilização desta política .....	2829
Detalhes da política .....	2829
Versão da política .....	2829
Documento da política JSON .....	2829
Saiba mais .....	2830

---

EC2InstanceProfileForImageBuilderECRContainerBuilds .....	2830
A utilização desta política .....	2831
Detalhes da política .....	2831
Versão da política .....	2831
Documento da política JSON .....	2831
Saiba mais .....	2832
ECRReplicationServiceRolePolicy .....	2833
A utilização desta política .....	2833
Detalhes da política .....	2833
Versão da política .....	2833
Documento da política JSON .....	2833
Saiba mais .....	2834
ElastiCacheServiceRolePolicy .....	2834
A utilização desta política .....	2834
Detalhes desta política .....	2834
Versão da política .....	2834
Documento da política JSON .....	2835
Saiba mais .....	2837
ElasticLoadBalancingFullAccess .....	2837
A utilização desta política .....	2837
Detalhes da política .....	2837
Versão da política .....	2837
Documento da política JSON .....	2837
Saiba mais .....	2839
ElasticLoadBalancingReadOnly .....	2839
Utilização desta política .....	2839
Detalhes desta política .....	2839
Versão da política .....	2839
Documento da política JSON .....	2840
Saiba mais .....	2841
ElementalActivationsDownloadSoftwareAccess .....	2841
A utilização desta política .....	2841
Detalhes da política .....	2841
Versão da política .....	2841
Documento da política JSON .....	2841
Saiba mais .....	2842



ElementalActivationsFullAccess .....	2842
A utilização desta política .....	2842
Detalhes da política .....	2842
Versão da política .....	2843
Documento da política JSON .....	2843
Saiba mais .....	2843
ElementalActivationsGenerateLicenses .....	2843
A utilização desta política .....	2844
Detalhes da política .....	2844
Versão da política .....	2844
Documento da política JSON .....	2844
Saiba mais .....	2845
ElementalActivationsReadOnlyAccess .....	2845
A utilização desta política .....	2845
Detalhes da política .....	2845
Versão da política .....	2845
Documento da política JSON .....	2845
Saiba mais .....	2846
ElementalAppliancesSoftwareFullAccess .....	2846
A utilização desta política .....	2846
Detalhes da política .....	2846
Versão da política .....	2847
Documento da política JSON .....	2847
Saiba mais .....	2847
ElementalAppliancesSoftwareReadOnlyAccess .....	2847
A utilização desta política .....	2848
Detalhes da política .....	2848
Versão da política .....	2848
Documento da política JSON .....	2848
Saiba mais .....	2848
ElementalSupportCenterFullAccess .....	2849
A utilização desta política .....	2849
Detalhes da política .....	2849
Versão da política .....	2849
Documento da política JSON .....	2849
Saiba mais .....	2850

EMRDescribeClusterPolicyForEMRWAL .....	2850
A utilização desta política .....	2850
Detalhes da política .....	2850
Versão da política .....	2851
Documento da política JSON .....	2851
Saiba mais .....	2851
FMSServiceRolePolicy .....	2851
A utilização desta política .....	2851
Detalhes da política .....	2852
Versão da política .....	2852
Documento da política JSON .....	2852
Saiba mais .....	2866
FSxDeleteServiceLinkedRoleAccess .....	2866
A utilização desta política .....	2866
Detalhes da política .....	2866
Versão da política .....	2867
Documento da política JSON .....	2867
Saiba mais .....	2867
GameLiftGameServerGroupPolicy .....	2867
A utilização desta política .....	2868
Detalhes da política .....	2868
Versão da política .....	2868
Documento da política JSON .....	2868
Saiba mais .....	2870
GlobalAcceleratorFullAccess .....	2870
A utilização desta política .....	2870
Detalhes da política .....	2870
Versão da política .....	2870
Documento da política JSON .....	2870
Saiba mais .....	2871
GlobalAcceleratorReadOnlyAccess .....	2872
A utilização desta política .....	2872
Detalhes da política .....	2872
Versão da política .....	2872
Documento da política JSON .....	2872
Saiba mais .....	2873

GreengrassOTAUpdateArtifactAccess .....	2873
A utilização desta política .....	2873
Detalhes da política .....	2873
Versão da política .....	2873
Documento da política JSON .....	2874
Saiba mais .....	2874
GroundTruthSyntheticConsoleFullAccess .....	2874
A utilização desta política .....	2875
Detalhes da política .....	2875
Versão da política .....	2875
Documento da política JSON .....	2875
Saiba mais .....	2875
GroundTruthSyntheticConsoleReadOnlyAccess .....	2876
A utilização desta política .....	2876
Detalhes da política .....	2876
Versão da política .....	2876
Documento da política JSON .....	2876
Saiba mais .....	2877
Health_OrganizationsServiceRolePolicy .....	2877
Utilização desta política .....	2877
Detalhes desta política .....	2877
Versão da política .....	2878
Documento da política JSON .....	2878
Saiba mais .....	2878
IAMAccessAdvisorReadOnly .....	2878
A utilização desta política .....	2879
Detalhes da política .....	2879
Versão da política .....	2879
Documento da política JSON .....	2879
Saiba mais .....	2880
IAMAccessAnalyzerFullAccess .....	2880
A utilização desta política .....	2880
Detalhes da política .....	2880
Versão da política .....	2881
Documento da política JSON .....	2881
Saiba mais .....	2882

IAMAccessAnalyzerReadOnlyAccess .....	2882
Utilização desta política .....	2882
Detalhes desta política .....	2882
Versão da política .....	2882
Documento da política JSON .....	2883
Saiba mais .....	2883
IAMFullAccess .....	2883
A utilização desta política .....	2884
Detalhes da política .....	2884
Versão da política .....	2884
Documento da política JSON .....	2884
Saiba mais .....	2885
IAMReadOnlyAccess .....	2885
A utilização desta política .....	2885
Detalhes da política .....	2885
Versão da política .....	2885
Documento da política JSON .....	2886
Saiba mais .....	2886
IAMSelfManageServiceSpecificCredentials .....	2886
A utilização desta política .....	2886
Detalhes da política .....	2887
Versão da política .....	2887
Documento da política JSON .....	2887
Saiba mais .....	2887
IAMUserChangePassword .....	2888
A utilização desta política .....	2888
Detalhes da política .....	2888
Versão da política .....	2888
Documento da política JSON .....	2888
Saiba mais .....	2889
IAMUserSSHKeys .....	2889
A utilização desta política .....	2889
Detalhes da política .....	2889
Versão da política .....	2890
Documento da política JSON .....	2890
Saiba mais .....	2890

IVSFullAccess .....	2891
Utilização desta política .....	2891
Detalhes desta política .....	2891
Versão da política .....	2891
Documento da política JSON .....	2891
Saiba mais .....	2892
IVSReadOnlyAccess .....	2892
Utilização desta política .....	2892
Detalhes desta política .....	2892
Versão da política .....	2892
Documento da política JSON .....	2893
Saiba mais .....	2894
IVSRecordToS3 .....	2894
A utilização desta política .....	2894
Detalhes da política .....	2894
Versão da política .....	2894
Documento da política JSON .....	2894
Saiba mais .....	2895
KafkaConnectServiceRolePolicy .....	2895
A utilização desta política .....	2895
Detalhes da política .....	2895
Versão da política .....	2896
Documento da política JSON .....	2896
Saiba mais .....	2897
KafkaServiceRolePolicy .....	2897
A utilização desta política .....	2897
Detalhes da política .....	2898
Versão da política .....	2898
Documento da política JSON .....	2898
Saiba mais .....	2899
KeyspacesReplicationServiceRolePolicy .....	2900
A utilização desta política .....	2900
Detalhes da política .....	2900
Versão da política .....	2900
Documento da política JSON .....	2900
Saiba mais .....	2901

LakeFormationDataAccessServiceRolePolicy .....	2901
Utilização desta política .....	2901
Detalhes desta política .....	2901
Versão da política .....	2901
Documento da política JSON .....	2902
Saiba mais .....	2902
LexBotPolicy .....	2902
A utilização desta política .....	2902
Detalhes da política .....	2902
Versão da política .....	2903
Documento da política JSON .....	2903
Saiba mais .....	2903
LexChannelPolicy .....	2904
A utilização desta política .....	2904
Detalhes da política .....	2904
Versão da política .....	2904
Documento da política JSON .....	2904
Saiba mais .....	2905
LightsailExportAccess .....	2905
A utilização desta política .....	2905
Detalhes da política .....	2905
Versão da política .....	2905
Documento da política JSON .....	2905
Saiba mais .....	2906
MediaConnectGatewayInstanceRolePolicy .....	2906
A utilização desta política .....	2907
Detalhes da política .....	2907
Versão da política .....	2907
Documento da política JSON .....	2907
Saiba mais .....	2908
MediaPackageServiceRolePolicy .....	2908
A utilização desta política .....	2908
Detalhes da política .....	2908
Versão da política .....	2908
Documento da política JSON .....	2908
Saiba mais .....	2909

MemoryDBServiceRolePolicy .....	2909
A utilização desta política .....	2909
Detalhes da política .....	2909
Versão da política .....	2910
Documento da política JSON .....	2910
Saiba mais .....	2912
MigrationHubDMSAccessServiceRolePolicy .....	2912
A utilização desta política .....	2912
Detalhes da política .....	2912
Versão da política .....	2912
Documento da política JSON .....	2913
Saiba mais .....	2914
MigrationHubServiceRolePolicy .....	2914
A utilização desta política .....	2914
Detalhes da política .....	2914
Versão da política .....	2914
Documento da política JSON .....	2914
Saiba mais .....	2916
MigrationHubSMSAccessServiceRolePolicy .....	2916
A utilização desta política .....	2916
Detalhes da política .....	2916
Versão da política .....	2916
Documento da política JSON .....	2917
Saiba mais .....	2917
MonitronServiceRolePolicy .....	2918
A utilização desta política .....	2918
Detalhes da política .....	2918
Versão da política .....	2918
Documento da política JSON .....	2918
Saiba mais .....	2919
NeptuneConsoleFullAccess .....	2919
Utilização desta política .....	2919
Detalhes desta política .....	2919
Versão da política .....	2919
Documento da política JSON .....	2920
Saiba mais .....	2925

NeptuneFullAccess .....	2925
Utilização desta política .....	2926
Detalhes desta política .....	2926
Versão da política .....	2926
Documento da política JSON .....	2926
Saiba mais .....	2930
NeptuneGraphReadOnlyAccess .....	2930
Utilização desta política .....	2930
Detalhes desta política .....	2930
Versão da política .....	2931
Documento da política JSON .....	2931
Saiba mais .....	2932
NeptuneReadOnlyAccess .....	2933
Utilização desta política .....	2933
Detalhes desta política .....	2933
Versão da política .....	2933
Documento da política JSON .....	2933
Saiba mais .....	2935
NetworkAdministrator .....	2936
A utilização desta política .....	2936
Detalhes da política .....	2936
Versão da política .....	2936
Documento da política JSON .....	2936
Saiba mais .....	2943
OAMFullAccess .....	2943
A utilização desta política .....	2943
Detalhes da política .....	2943
Versão da política .....	2943
Documento da política JSON .....	2944
Saiba mais .....	2944
OAMReadOnlyAccess .....	2944
A utilização desta política .....	2944
Detalhes da política .....	2944
Versão da política .....	2945
Documento da política JSON .....	2945
Saiba mais .....	2945



PartnerCentralAccountManagementUserRoleAssociation .....	2946
Utilização desta política .....	2946
Detalhes desta política .....	2946
Versão da política .....	2946
Documento da política JSON .....	2946
Saiba mais .....	2947
PowerUserAccess .....	2947
A utilização desta política .....	2947
Detalhes da política .....	2947
Versão da política .....	2948
Documento da política JSON .....	2948
Saiba mais .....	2949
QuickSightAccessForS3StorageManagementAnalyticsReadOnly .....	2949
A utilização desta política .....	2949
Detalhes da política .....	2949
Versão da política .....	2949
Documento da política JSON .....	2950
Saiba mais .....	2950
RDSCloudHsmAuthorizationRole .....	2950
A utilização desta política .....	2951
Detalhes da política .....	2951
Versão da política .....	2951
Documento da política JSON .....	2951
Saiba mais .....	2952
ReadOnlyAccess .....	2952
Utilização desta política .....	2952
Detalhes desta política .....	2952
Versão da política .....	2952
Documento da política JSON .....	2952
Saiba mais .....	2999
ResourceGroupsandTagEditorFullAccess .....	2999
A utilização desta política .....	2999
Detalhes da política .....	2999
Versão da política .....	2999
Documento da política JSON .....	3000
Saiba mais .....	3000

ResourceGroupsandTagEditorReadOnlyAccess .....	3000
A utilização desta política .....	3001
Detalhes da política .....	3001
Versão da política .....	3001
Documento da política JSON .....	3001
Saiba mais .....	3002
ResourceGroupsServiceRolePolicy .....	3002
A utilização desta política .....	3002
Detalhes da política .....	3002
Versão da política .....	3002
Documento da política JSON .....	3003
Saiba mais .....	3003
ROSAAmazonEBSCSIDriverOperatorPolicy .....	3003
A utilização desta política .....	3003
Detalhes da política .....	3003
Versão da política .....	3004
Documento da política JSON .....	3004
Saiba mais .....	3007
ROSACloudNetworkConfigOperatorPolicy .....	3007
A utilização desta política .....	3007
Detalhes da política .....	3007
Versão da política .....	3008
Documento da política JSON .....	3008
Saiba mais .....	3009
ROSAControlPlaneOperatorPolicy .....	3009
A utilização desta política .....	3009
Detalhes da política .....	3009
Versão da política .....	3009
Documento da política JSON .....	3010
Saiba mais .....	3014
ROSAImageRegistryOperatorPolicy .....	3014
Utilização desta política .....	3014
Detalhes desta política .....	3014
Versão da política .....	3015
Documento da política JSON .....	3015
Saiba mais .....	3016

ROSAIngressOperatorPolicy .....	3016
A utilização desta política .....	3017
Detalhes da política .....	3017
Versão da política .....	3017
Documento da política JSON .....	3017
Saiba mais .....	3018
ROSAInstallerPolicy .....	3018
Utilização desta política .....	3018
Detalhes desta política .....	3018
Versão da política .....	3019
Documento da política JSON .....	3019
Saiba mais .....	3026
ROSAKMSProviderPolicy .....	3026
A utilização desta política .....	3026
Detalhes da política .....	3026
Versão da política .....	3027
Documento da política JSON .....	3027
Saiba mais .....	3027
ROSAKubeControllerPolicy .....	3028
A utilização desta política .....	3028
Detalhes da política .....	3028
Versão da política .....	3028
Documento da política JSON .....	3028
Saiba mais .....	3033
ROSAManageSubscription .....	3033
A utilização desta política .....	3033
Detalhes da política .....	3033
Versão da política .....	3033
Documento da política JSON .....	3034
Saiba mais .....	3034
ROSANodePoolManagementPolicy .....	3035
A utilização desta política .....	3035
Detalhes da política .....	3035
Versão da política .....	3035
Documento da política JSON .....	3035
Saiba mais .....	3041

ROSASRESupportPolicy .....	3041
Utilização desta política .....	3041
Detalhes desta política .....	3041
Versão da política .....	3042
Documento da política JSON .....	3042
Saiba mais .....	3047
ROSAWorkerInstancePolicy .....	3047
A utilização desta política .....	3047
Detalhes da política .....	3047
Versão da política .....	3047
Documento da política JSON .....	3048
Saiba mais .....	3048
Route53RecoveryReadinessServiceRolePolicy .....	3048
A utilização desta política .....	3048
Detalhes da política .....	3048
Versão da política .....	3049
Documento da política JSON .....	3049
Saiba mais .....	3052
Route53ResolverServiceRolePolicy .....	3053
A utilização desta política .....	3053
Detalhes da política .....	3053
Versão da política .....	3053
Documento da política JSON .....	3053
Saiba mais .....	3054
S3StorageLensServiceRolePolicy .....	3054
A utilização desta política .....	3054
Detalhes da política .....	3054
Versão da política .....	3054
Documento da política JSON .....	3055
Saiba mais .....	3055
SecretsManagerReadWrite .....	3055
Utilização desta política .....	3056
Detalhes desta política .....	3056
Versão da política .....	3056
Documento da política JSON .....	3056
Saiba mais .....	3058

SecurityAudit .....	3058
Utilização desta política .....	3058
Detalhes desta política .....	3058
Versão da política .....	3058
Documento da política JSON .....	3059
Saiba mais .....	3074
SecurityLakeServiceLinkedRole .....	3074
Utilização desta política .....	3075
Detalhes desta política .....	3075
Versão da política .....	3075
Documento da política JSON .....	3075
Saiba mais .....	3078
ServerMigration_ServiceRole .....	3078
A utilização desta política .....	3078
Detalhes da política .....	3078
Versão da política .....	3078
Documento da política JSON .....	3078
Saiba mais .....	3083
ServerMigrationConnector .....	3083
A utilização desta política .....	3084
Detalhes da política .....	3084
Versão da política .....	3084
Documento da política JSON .....	3084
Saiba mais .....	3086
ServerMigrationServiceConsoleFullAccess .....	3086
A utilização desta política .....	3086
Detalhes da política .....	3086
Versão da política .....	3086
Documento da política JSON .....	3086
Saiba mais .....	3088
ServerMigrationServiceLaunchRole .....	3088
A utilização desta política .....	3088
Detalhes da política .....	3089
Versão da política .....	3089
Documento da política JSON .....	3089
Saiba mais .....	3092

ServerMigrationServiceRoleForInstanceValidation .....	3092
A utilização desta política .....	3092
Detalhes da política .....	3092
Versão da política .....	3092
Documento da política JSON .....	3093
Saiba mais .....	3093
ServiceQuotasFullAccess .....	3093
A utilização desta política .....	3093
Detalhes da política .....	3094
Versão da política .....	3094
Documento da política JSON .....	3094
Saiba mais .....	3096
ServiceQuotasReadOnlyAccess .....	3096
A utilização desta política .....	3096
Detalhes da política .....	3096
Versão da política .....	3096
Documento da política JSON .....	3096
Saiba mais .....	3097
ServiceQuotasServiceRolePolicy .....	3098
A utilização desta política .....	3098
Detalhes da política .....	3098
Versão da política .....	3098
Documento da política JSON .....	3098
Saiba mais .....	3099
SimpleWorkflowFullAccess .....	3099
A utilização desta política .....	3099
Detalhes da política .....	3099
Versão da política .....	3099
Documento da política JSON .....	3100
Saiba mais .....	3100
SupportUser .....	3100
A utilização desta política .....	3100
Detalhes da política .....	3100
Versão da política .....	3101
Documento da política JSON .....	3101
Saiba mais .....	3106

SystemAdministrator .....	3106
A utilização desta política .....	3106
Detalhes da política .....	3106
Versão da política .....	3106
Documento da política JSON .....	3107
Saiba mais .....	3113
TranslateFullAccess .....	3113
A utilização desta política .....	3113
Detalhes da política .....	3113
Versão da política .....	3113
Documento da política JSON .....	3113
Saiba mais .....	3114
TranslateReadOnly .....	3114
A utilização desta política .....	3114
Detalhes da política .....	3114
Versão da política .....	3115
Documento da política JSON .....	3115
Saiba mais .....	3115
ViewOnlyAccess .....	3116
A utilização desta política .....	3116
Detalhes da política .....	3116
Versão da política .....	3116
Documento da política JSON .....	3116
Saiba mais .....	3122
VMImportExportRoleForAWSConnector .....	3122
A utilização desta política .....	3123
Detalhes da política .....	3123
Versão da política .....	3123
Documento da política JSON .....	3123
Saiba mais .....	3124
VPCLatticeFullAccess .....	3124
A utilização desta política .....	3124
Detalhes da política .....	3124
Versão da política .....	3124
Documento da política JSON .....	3125
Saiba mais .....	3127

VPCLatticeReadOnlyAccess .....	3127
A utilização desta política .....	3127
Detalhes da política .....	3127
Versão da política .....	3127
Documento da política JSON .....	3127
Saiba mais .....	3128
VPCLatticeServicesInvokeAccess .....	3129
A utilização desta política .....	3129
Detalhes da política .....	3129
Versão da política .....	3129
Documento da política JSON .....	3129
Saiba mais .....	3130
WAFLoggingServiceRolePolicy .....	3130
A utilização desta política .....	3130
Detalhes da política .....	3130
Versão da política .....	3130
Documento da política JSON .....	3130
Saiba mais .....	3131
WAFRegionalLoggingServiceRolePolicy .....	3131
A utilização desta política .....	3131
Detalhes da política .....	3131
Versão da política .....	3132
Documento da política JSON .....	3132
Saiba mais .....	3132
WAFV2LoggingServiceRolePolicy .....	3132
A utilização desta política .....	3133
Detalhes da política .....	3133
Versão da política .....	3133
Documento da política JSON .....	3133
Saiba mais .....	3134
WellArchitectedConsoleFullAccess .....	3134
A utilização desta política .....	3134
Detalhes da política .....	3134
Versão da política .....	3134
Documento da política JSON .....	3134
Saiba mais .....	3135



---

WellArchitectedConsoleReadOnlyAccess .....	3135
A utilização desta política .....	3135
Detalhes da política .....	3135
Versão da política .....	3136
Documento da política JSON .....	3136
Saiba mais .....	3136
WorkLinkServiceRolePolicy .....	3136
A utilização desta política .....	3137
Detalhes da política .....	3137
Versão da política .....	3137
Documento da política JSON .....	3137
Saiba mais .....	3138
.....	mmmcxxxix

# O que são as políticas gerenciadas pela AWS?

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são projetadas para conceder permissões em muitos cenários de uso comum. Elas simplificam o processo de conceder permissões aos usuários, grupos e funções, comparados à elaboração manual de políticas.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso por todos os clientes da AWS. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente da](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Caso a AWS faça atualizações nas permissões estabelecidas em uma política gerenciada pela AWS, estas mudanças impactarão todas as identidades das entidades principais (usuários, grupos e funções) vinculadas à esta política. A AWS é mais propensa a atualizar uma política gerenciada pela AWS durante o lançamento de um novo serviço da AWS ou quando novas operações de API estiverem disponíveis para serviços existentes.

Para informações adicionais, consulte as [Políticas Gerenciadas pela AWS](#) na Guia do Usuário do IAM.

## Compreender as páginas de referência de políticas

Cada página de referência de política fornece as seguintes informações:

- Utilização desta política: indica se é possível vincular esta política a usuários, grupos e funções
- Detalhes desta política
  - Tipo: o tipo de política gerenciada pela AWS
    - `AWS managed policy`: uma política padrão gerenciada pela AWS
    - `Job function policy` – Política alinhada com as funções comuns do setor
    - `Service-linked role policy` – Política que está vinculada a uma função associada a um serviço, possibilitando que um serviço execute ações em seu nome, tais como [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
    - `Service role policy` – Política elaborada para ser compatível com funções de serviço, tais como [the section called “AWSControlTowerServiceRolePolicy”](#)

- Horário de criação — Quando a política foi criada pela primeira vez
- Hora da edição — Quando essa versão da política foi editada
- ARN – O nome do recurso da Amazon (ARN) da política em questão
- Versão da política — A versão das permissões que foram concedidas pela política
- Documento da política JSON — A política JSON
- Saiba mais — Links para a documentação relacionada às políticas gerenciadas pela AWS

## Políticas gerenciadas pela AWS obsoletas

A AWS atualiza regularmente as políticas gerenciadas pela AWS. Na maioria dos casos, incluímos permissões em uma política. Isto acontece quando lançamos um novo serviço ou atributo. Visando reforçar a segurança das políticas gerenciadas pela AWS, ocasionalmente restringimos o escopo dessas políticas. Ao remover as permissões de uma política, marcamos a política como obsoleta e disponibilizamos uma nova versão. No caso de a AWS descontinuar um serviço ou um atributo, também encerraremos a política gerenciada pela AWS associada a este recurso.

Se você receber um aviso por e-mail de que uma política que está utilizando tornou-se obsoleta, é altamente recomendado que tome medidas imediatamente. Identifique as alterações na política e atualize os seus fluxos de trabalho. Se a AWS oferecer uma política de substituição, planeje vinculá-la a todas as identidades afetadas (usuários, grupos e funções) e, posteriormente, desvincular a política obsoleta destas identidades.

Uma política obsoleta tem as seguintes características:

- Ela foi removida deste guia.
- Ela mantém as permissões operacionais para todas as identidades atualmente vinculadas.
- Nas contas em que a política está vinculada a uma identidade, ela é exibida na lista de Políticas no console do IAM com um ícone de aviso ao lado.
- Não é possível associá-la a nenhuma nova identidade. Se você desvinculá-la de uma identidade existente, não será possível reestabelecer esta conexão.
- Após desvinculá-la de todas as entidades atuais, ela deixará de ser visível.

# AWS políticas gerenciadas

## AWS políticas gerenciadas

- [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](#)
- [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](#)
- [AmazonEC2ContainerServiceforEC2Role](#)
- [AmazonEC2ContainerServiceRole](#)
- [AmazonEC2FullAccess](#)

- [AmazonEC2ReadOnlyAccess](#)
- [AmazonEC2RoleforAWSCodeDeploy](#)
- [AmazonEC2RoleforAWSCodeDeployLimited](#)
- [AmazonEC2RoleforDataPipelineRole](#)
- [AmazonEC2RoleforSSM](#)
- [AmazonEC2RolePolicyForLaunchWizard](#)
- [AmazonEC2SpotFleetAutoscaleRole](#)
- [AmazonEC2SpotFleetTaggingRole](#)
- [AmazonECS\\_FullAccess](#)
- [AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity](#)
- [AmazonECSInfrastructureRolePolicyForVolumes](#)
- [AmazonECSServiceRolePolicy](#)
- [AmazonECSTaskExecutionRolePolicy](#)
- [AmazonEFSCSIDriverPolicy](#)
- [AmazonEKS\\_CNI\\_Policy](#)
- [AmazonEKSClusterPolicy](#)
- [AmazonEKSConectorServiceRolePolicy](#)
- [AmazonEKSFargatePodExecutionRolePolicy](#)
- [AmazonEKSTaskExecutionRolePolicy](#)
- [AmazonEKSLocalOutpostClusterPolicy](#)
- [AmazonEKSLocalOutpostServiceRolePolicy](#)
- [AmazonEKSServicePolicy](#)
- [AmazonEKSServiceRolePolicy](#)
- [AmazonEKSVPCResourceController](#)
- [AmazonEKSWorkerNodePolicy](#)
- [AmazonElastiCacheFullAccess](#)
- [AmazonElastiCacheReadOnlyAccess](#)
- [AmazonElasticContainerRegistryPublicFullAccess](#)
- [AmazonElasticContainerRegistryPublicPowerUser](#)



- [AmazonElasticContainerRegistryPublicReadOnly](#)
- [AmazonElasticFileSystemClientFullAccess](#)
- [AmazonElasticFileSystemClientReadOnlyAccess](#)
- [AmazonElasticFileSystemClientReadWriteAccess](#)
- [AmazonElasticFileSystemFullAccess](#)
- [AmazonElasticFileSystemReadOnlyAccess](#)
- [AmazonElasticFileSystemServiceRolePolicy](#)
- [AmazonElasticFileSystemsUtils](#)
- [AmazonElasticMapReduceEditorsRole](#)
- [AmazonElasticMapReduceforAutoScalingRole](#)
- [AmazonElasticMapReduceforEC2Role](#)
- [AmazonElasticMapReduceFullAccess](#)
- [AmazonElasticMapReducePlacementGroupPolicy](#)
- [AmazonElasticMapReduceReadOnlyAccess](#)
- [AmazonElasticMapReduceRole](#)
- [AmazonElasticsearchServiceRolePolicy](#)
- [AmazonElasticTranscoder\\_FullAccess](#)
- [AmazonElasticTranscoder\\_JobsSubmitter](#)
- [AmazonElasticTranscoder\\_ReadOnlyAccess](#)
- [AmazonElasticTranscoderRole](#)
- [AmazonEMRCleanupPolicy](#)
- [AmazonEMRContainersServiceRolePolicy](#)
- [AmazonEMRFullAccessPolicy\\_v2](#)
- [AmazonEMRReadOnlyAccessPolicy\\_v2](#)
- [AmazonEMRServerlessServiceRolePolicy](#)
- [AmazonEMRServicePolicy\\_v2](#)
- [AmazonESCognitoAccess](#)
- [AmazonESFullAccess](#)
- [AmazonESReadOnlyAccess](#)

- [AmazonEventBridgeApiDestinationsServiceRolePolicy](#)
- [AmazonEventBridgeFullAccess](#)
- [AmazonEventBridgePipesFullAccess](#)
- [AmazonEventBridgePipesOperatorAccess](#)
- [AmazonEventBridgePipesReadOnlyAccess](#)
- [AmazonEventBridgeReadOnlyAccess](#)
- [AmazonEventBridgeSchedulerFullAccess](#)
- [AmazonEventBridgeSchedulerReadOnlyAccess](#)
- [AmazonEventBridgeSchemasFullAccess](#)
- [AmazonEventBridgeSchemasReadOnlyAccess](#)
- [AmazonEventBridgeSchemasServiceRolePolicy](#)
- [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](#)
- [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](#)
- [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](#)
- [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](#)
- [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](#)
- [AWSDeepLensLambdaFunctionAccessPolicy](#)
- [AWSDeepLensServiceRolePolicy](#)
- [AWSDeepRacerAccountAdminAccess](#)
- [AWSDeepRacerCloudFormationAccessPolicy](#)
- [AWSDeepRacerDefaultMultiUserAccess](#)
- [AWSDeepRacerFullAccess](#)
- [AWSDeepRacerRoboMakerAccessPolicy](#)
- [AWSDeepRacerServiceRolePolicy](#)
- [AWSDenyAll](#)
- [AWSDeviceFarmFullAccess](#)
- [AWSDeviceFarmServiceRolePolicy](#)
- [AWSDeviceFarmTestGridServiceRolePolicy](#)
- [AWSDirectConnectFullAccess](#)
- [AWSDirectConnectReadOnlyAccess](#)
- [AWSDirectConnectServiceRolePolicy](#)
- [AWSDirectoryServiceFullAccess](#)
- [AWSDirectoryServiceReadOnlyAccess](#)
- [AWSDiscoveryContinuousExportFirehosePolicy](#)

- [AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWSDMSServerlessServiceRolePolicy](#)
- [AWSEC2CapacityReservationFleetRolePolicy](#)
- [AWSEC2FleetServiceRolePolicy](#)
- [AWSEC2SpotFleetServiceRolePolicy](#)
- [AWSEC2SpotServiceRolePolicy](#)
- [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](#)
- [AWSIoTTwinMakerServiceRolePolicy](#)
- [AWSIoTWirelessDataAccess](#)
- [AWSIoTWirelessFullAccess](#)
- [AWSIoTWirelessFullPublishAccess](#)
- [AWSIoTWirelessGatewayCertManager](#)
- [AWSIoTWirelessLogging](#)
- [AWSIoTWirelessReadOnlyAccess](#)
- [AWSIPAMServiceRolePolicy](#)
- [AWSIQContractServiceRolePolicy](#)
- [AWSIQFullAccess](#)
- [AWSIQPermissionServiceRolePolicy](#)
- [AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy](#)

- [AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy](#)
- [AWSKeyManagementServicePowerUser](#)
- [AWSLakeFormationCrossAccountManager](#)
- [AWSLakeFormationDataAdmin](#)
- [AWSLambda\\_FullAccess](#)
- [AWSLambda\\_ReadOnlyAccess](#)
- [AWSLambdaBasicExecutionRole](#)
- [AWSLambdaDynamoDBExecutionRole](#)
- [AWSLambdaENIManagementAccess](#)
- [AWSLambdaExecute](#)
- [AWSLambdaFullAccess](#)
- [AWSLambdaInvocation-DynamoDB](#)
- [AWSLambdaKinesisExecutionRole](#)
- [AWSLambdaMSKExecutionRole](#)
- [AWSLambdaReplicator](#)
- [AWSLambdaRole](#)
- [AWSLambdaSQSQueueExecutionRole](#)
- [AWSLambdaVPCAccessExecutionRole](#)
- [AWSLicenseManagerConsumptionPolicy](#)
- [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)
- [AWSLicenseManagerMasterAccountRolePolicy](#)
- [AWSLicenseManagerMemberAccountRolePolicy](#)
- [AWSLicenseManagerServiceRolePolicy](#)
- [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)
- [AWSM2ServicePolicy](#)
- [AWSManagedServices\\_ContactsServiceRolePolicy](#)
- [AWSManagedServices\\_DetectiveControlsConfig\\_ServiceRolePolicy](#)
- [AWSManagedServices\\_EventsServiceRolePolicy](#)
- [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](#)

- [AWSPublicCAAuditor](#)
- [AWSPublicCAFullAccess](#)
- [AWSPublicCAPrivilegedUser](#)
- [AWSPublicCARedOnly](#)
- [AWSPublicCAUser](#)
- [AWSPublicMarketplaceAdminFullAccess](#)
- [AWSPublicMarketplaceRequests](#)
- [AWSPublicNetworksServiceRolePolicy](#)
- [AWSPublicProtonCodeBuildProvisioningBasicAccess](#)
- [AWSPublicProtonCodeBuildProvisioningServiceRolePolicy](#)
- [AWSPublicProtonDeveloperAccess](#)
- [AWSPublicProtonFullAccess](#)
- [AWSPublicProtonReadOnlyAccess](#)
- [AWSPublicProtonServiceGitSyncServiceRolePolicy](#)
- [AWSPublicProtonSyncServiceRolePolicy](#)
- [AWSPublicPurchaseOrdersServiceRolePolicy](#)
- [AWSPublicQuicksightAthenaAccess](#)
- [AWSPublicQuickSightDescribeRDS](#)
- [AWSPublicQuickSightDescribeRedshift](#)
- [AWSPublicQuickSightElasticsearchPolicy](#)
- [AWSPublicQuickSightIoTAnalyticsAccess](#)
- [AWSPublicQuickSightListIAM](#)
- [AWSPublicQuicksightOpenSearchPolicy](#)
- [AWSPublicQuickSightSageMakerPolicy](#)
- [AWSPublicQuickSightTimestreamPolicy](#)
- [AWSPublicReachabilityAnalyzerServiceRolePolicy](#)
- [AWSPublicRefactoringToolkitFullAccess](#)
- [AWSPublicRefactoringToolkitSidecarPolicy](#)
- [AWSPublicrePostPrivateCloudWatchAccess](#)
- [AWSPublicRepostSpaceSupportOperationsPolicy](#)

- [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](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy](#)
- [AWSServiceRoleForCloudWatchMetrics\\_DbPerfInsightsServiceRolePolicy](#)
- [AWSServiceRoleForCodeGuru-Profiler](#)
- [AWSServiceRoleForCodeWhispererPolicy](#)
- [AWSServiceRoleForEC2ScheduledInstances](#)
- [AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy](#)
- [AWSServiceRoleForImageBuilder](#)
- [AWSServiceRoleForIoTSiteWise](#)
- [AWSServiceRoleForLogDeliveryPolicy](#)
- [AWSServiceRoleForMonitronPolicy](#)
- [AWSServiceRoleForNeptuneGraphPolicy](#)
- [AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWSServiceRoleForSMS](#)
- [AWSServiceRolePolicyForBackupReports](#)
- [AWSServiceRolePolicyForBackupRestoreTesting](#)
- [AWSShieldDRTAccessPolicy](#)
- [AWSShieldServiceRolePolicy](#)
- [AWSSSMForSAPServiceLinkedRolePolicy](#)
- [AWSSSMOpsInsightsServiceRolePolicy](#)
- [AWSSSODirectoryAdministrator](#)
- [AWSSSODirectoryReadOnly](#)
- [AWSSSOMasterAccountAdministrator](#)
- [AWSSSOMemberAccountAdministrator](#)
- [AWSSSOReadOnly](#)
- [AWSSSOServiceRolePolicy](#)
- [AWSSStepFunctionsConsoleFullAccess](#)
- [AWSSStepFunctionsFullAccess](#)
- [AWSSStepFunctionsReadOnlyAccess](#)

- [AWStorageGatewayFullAccess](#)
- [AWStorageGatewayReadOnlyAccess](#)
- [AWStorageGatewayServiceRolePolicy](#)
- [AWSupplyChainFederationAdminAccess](#)
- [AWSupportAccess](#)
- [AWSupportAppFullAccess](#)
- [AWSupportAppReadOnlyAccess](#)
- [AWSupportPlansFullAccess](#)
- [AWSupportPlansReadOnlyAccess](#)
- [AWSupportServiceRolePolicy](#)
- [AWSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSystemsManagerChangeManagementServicePolicy](#)
- [AWSystemsManagerForSAPFullAccess](#)
- [AWSystemsManagerForSAPReadOnlyAccess](#)
- [AWSystemsManagerOpsDataSyncServiceRolePolicy](#)
- [AWThinkboxAssetServerPolicy](#)
- [AWThinkboxAWSPortalAdminPolicy](#)
- [AWThinkboxAWSPortalGatewayPolicy](#)
- [AWThinkboxAWSPortalWorkerPolicy](#)
- [AWThinkboxDeadlineResourceTrackerAccessPolicy](#)
- [AWThinkboxDeadlineResourceTrackerAdminPolicy](#)
- [AWThinkboxDeadlineSpotEventPluginAdminPolicy](#)
- [AWThinkboxDeadlineSpotEventPluginWorkerPolicy](#)
- [AWTransferConsoleFullAccess](#)
- [AWTransferFullAccess](#)
- [AWTransferLoggingAccess](#)
- [AWTransferReadOnlyAccess](#)
- [AWTrustedAdvisorPriorityFullAccess](#)
- [AWTrustedAdvisorPriorityReadOnlyAccess](#)
- [AWTrustedAdvisorReportingServiceRolePolicy](#)

- [AWS TrustedAdvisorServiceRolePolicy](#)
- [AWS UserNotificationsServiceLinkedRolePolicy](#)
- [AWS VendorInsightsAssessorFullAccess](#)
- [AWS VendorInsightsAssessorReadOnly](#)
- [AWS VendorInsightsVendorFullAccess](#)
- [AWS VendorInsightsVendorReadOnly](#)
- [AWS VpcLatticeServiceRolePolicy](#)
- [AWS VPCS2SVpnServiceRolePolicy](#)
- [AWS VPCTransitGatewayServiceRolePolicy](#)
- [AWS VPCVerifiedAccessServiceRolePolicy](#)
- [AWS WAFConsoleFullAccess](#)
- [AWS WAFConsoleReadOnlyAccess](#)
- [AWS WAFFullAccess](#)
- [AWS WAFReadOnlyAccess](#)
- [AWS WellArchitectedDiscoveryServiceRolePolicy](#)
- [AWS WellArchitectedOrganizationsServiceRolePolicy](#)
- [AWS WickrFullAccess](#)
- [AWS XrayCrossAccountSharingConfiguration](#)
- [AWS XRayDaemonWriteAccess](#)
- [AWS XrayFullAccess](#)
- [AWS XrayReadOnlyAccess](#)
- [AWS XrayWriteOnlyAccess](#)
- [AWS ZonalAutoshiftPracticeRunSLRPolicy](#)
- [BatchServiceRolePolicy](#)
- [Billing](#)
- [CertificateManagerServiceRolePolicy](#)
- [ClientVPNServiceConnectionsRolePolicy](#)
- [ClientVPNServiceRolePolicy](#)
- [CloudFormationStackSetsOrgAdminServiceRolePolicy](#)
- [CloudFormationStackSetsOrgMemberServiceRolePolicy](#)

- [CloudFrontFullAccess](#)
- [CloudFrontReadOnlyAccess](#)
- [CloudHSMServiceRolePolicy](#)
- [CloudSearchFullAccess](#)
- [CloudSearchReadOnlyAccess](#)
- [CloudTrailServiceRolePolicy](#)
- [CloudWatch-CrossAccountAccess](#)
- [CloudWatchActionsEC2Access](#)
- [CloudWatchAgentAdminPolicy](#)
- [CloudWatchAgentServerPolicy](#)
- [CloudWatchApplicationInsightsFullAccess](#)
- [CloudWatchApplicationInsightsReadOnlyAccess](#)
- [CloudwatchApplicationInsightsServiceLinkedRolePolicy](#)
- [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](#)
- [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](#)
- [PartnerCentralAccountManagementUserRoleAssociation](#)
- [PowerUserAccess](#)
- [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](#)
- [SupportUser](#)
- [SystemAdministrator](#)
- [TranslateFullAccess](#)
- [TranslateReadOnly](#)
- [ViewOnlyAccess](#)

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

## AccessAnalyzerServiceRolePolicy

A `AccessAnalyzerServiceRolePolicy` é uma [política gerenciada pela AWS](#) que: permite que o Access Analyzer analise os metadados do recurso

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de dezembro de 2019, 17:13 UTC
- Horário editado: 22 de janeiro de 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

### Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr: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",
        "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" : "*"
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AdministratorAccess

AdministratorAccess é uma [política AWS gerenciada](#) que: fornece acesso total aos AWS serviços e recursos.

### Utilização desta política

Você pode vincular a AdministratorAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Hora da edição: 06 de fevereiro de 2015, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AdministratorAccess-Amplify

AdministratorAccess-Amplify é uma [política gerenciada da AWS](#) que outorga permissões administrativas à conta e, simultaneamente, autoriza explicitamente o acesso direto aos recursos essenciais para os aplicativos Amplify.

## A utilização desta política

Você pode vincular a AdministratorAccess-Amplify aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 19:03 UTC



- Horário de edição: 31 de maio de 2023, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation>ListStacks",
        "cloudformation>ListStackResources",
        "cloudformation>DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet"
      ],
      "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:*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AdministratorAccess-AWSElasticBeanstalk

AdministratorAccess-AWSElasticBeanstalk é uma [política gerenciada da AWS](#) que: concede permissões administrativas à conta. Permite explicitamente que desenvolvedores e administradores obtenham acesso direto aos recursos de que precisam para gerenciar os aplicativos da AWS Elastic Beanstalk

## A utilização desta política

Você pode vincular a `AdministratorAccess-AWSElasticBeanstalk` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de janeiro de 2021, 19:36 UTC
- Horário de edição: 23 de março de 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",

```

```

    "codecommit:Get*",
    "codecommit:UploadArchive",
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
    "ec2:AuthorizeSecurityGroup*",
    "ec2:CreateLaunchTemplate*",
    "ec2:CreateSecurityGroup",
    "ec2:CreateTags",
    "ec2>DeleteLaunchTemplate*",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTags",
    "ec2:Describe*",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroup*",
    "ecs:CreateCluster",
    "ecs:DeRegisterTaskDefinition",
    "ecs:Describe*",
    "ecs:List*",
    "ecs:RegisterTaskDefinition",
    "elasticbeanstalk:*",
    "elasticloadbalancing:Describe*",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListServerCertificates",
    "logs:Describe*",
    "rds:Describe*",
    "s3:ListAllMyBuckets",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:*"
  ],
  "Resource" : [

```

```

    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
**",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CancelUpdateStack",
    "cloudformation:ContinueUpdateRollback",
    "cloudformation>CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation>ListStackResources",
    "cloudformation:SignalResource",
    "cloudformation:TagResource",
    "cloudformation:UntagResource",
    "cloudformation:UpdateStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch>DeleteAlarms",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:awseb-*",
    "arn:aws:cloudwatch:*:*:alarm:eb-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codebuild:BatchGetBuilds",
    "codebuild>CreateProject",
    "codebuild>DeleteProject",
    "codebuild:StartBuild"
  ]
}

```

```

    ],
    "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:CreateTable",
      "dynamodb>DeleteTable",
      "dynamodb:DescribeTable",
      "dynamodb:TagResource"
    ],
    "Resource" : [
      "arn:aws:dynamodb:*:*:table/awseb-e-*",
      "arn:aws:dynamodb:*:*:table/eb-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RebootInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" : [
          "arn:aws:cloudformation:*:*:stack/awseb-e-*",
          "arn:aws:cloudformation:*:*:stack/eb-*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Effect" : "Allow",

```

```

    "Action" : [
      "ecs:DeleteCluster"
    ],
    "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:*Rule",
      "elasticloadbalancing:*Tags",
      "elasticloadbalancing:SetRulePriorities",
      "elasticloadbalancing:SetSecurityGroups"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:*"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
      "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
      "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AddRoleToInstanceProfile",
      "iam:CreateInstanceProfile",

```



```
    "iam:CreateRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-elasticbeanstalk*",
    "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:AttachRolePolicy"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
  "Condition" : {
    "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"
      ]
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AlexaForBusinessDeviceSetup

AlexaForBusinessDeviceSetup é uma [política gerenciada da AWS](#) que: fornece acesso à configuração do dispositivo aos serviços de AlexaForBusiness

## A utilização desta política

Você pode vincular a AlexaForBusinessDeviceSetup aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:47 UTC
- Horário de edição: 20 de maio de 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "A4bDeviceSetupAccess",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessFullAccess

AlexaForBusinessFullAccess é uma [política gerenciada da AWS](#) que: concede acesso total aos recursos do AlexaForBusiness e acesso a atributos relacionados Serviços da AWS

### A utilização desta política

Você pode vincular a AlexaForBusinessFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:47 UTC
- Horário de edição: 01 de julho de 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessGatewayExecution

AlexaForBusinessGatewayExecution é uma [política gerenciada da AWS](#) que: fornece acesso de execução de gateway aos serviços AlexaForBusiness

## A utilização desta política

Você pode vincular a `AlexaForBusinessGatewayExecution` aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:47 UTC
- Horário de edição: 30 de novembro de 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "a4b:List*",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogGroups",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessLifesizeDelegatedAccessPolicy

AlexaForBusinessLifesizeDelegatedAccessPolicy é uma [política gerenciada da AWS](#) que: fornece acesso aos dispositivos Lifesize AVS

### A utilização desta política

Você pode vincular a AlexaForBusinessLifesizeDelegatedAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de junho de 2020, 19:46 UTC
- Horário de edição: 12 de junho de 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessNetworkProfileServicePolicy

AlexaForBusinessNetworkProfileServicePolicy é uma [política gerenciada da AWS](#) que: essa política permite que o Alexa for Business execute tarefas automatizadas agendadas pelos seus perfis de rede.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 13 de março de 2019, 00:53 UTC
- Horário de edição: 5 de abril de 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessPolyDelegatedAccessPolicy

AlexaForBusinessPolyDelegatedAccessPolicy é uma [política gerenciada da AWS](#) que fornece acesso aos dispositivos Poly AVS

### A utilização desta política

Você pode vincular a AlexaForBusinessPolyDelegatedAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de outubro de 2019, 19:48 UTC
- Horário de edição: 16 de outubro de 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AlexaForBusinessReadOnlyAccess

AlexaForBusinessReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornecer acesso somente de leitura aos serviços do AlexaForBusiness

## A utilização desta política

Você pode vincular a `AlexaForBusinessReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:47 UTC
- Horário de edição: 20 de novembro de 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAPIGatewayAdministrator

AmazonAPIGatewayAdministrator é uma [política gerenciada da AWS](#) que: fornece acesso total para criar/editar/excluir APIs no Amazon API Gateway por meio de AWS Management Console

### A utilização desta política

Você pode vincular a AmazonAPIGatewayAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:34 UTC
- Horário de edição: 09 de julho de 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAPIGatewayInvokeFullAccess

AmazonAPIGatewayInvokeFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total para acessar APIs no Amazon API Gateway.

### A utilização desta política

Você pode vincular a AmazonAPIGatewayInvokeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:36 UTC
- Horário de edição: 18 de dezembro de 2018, 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogs é uma [política gerenciada da AWS](#) que: permite que o API Gateway envie registros para a conta do usuário.

### A utilização desta política

Você pode vincular a AmazonAPIGatewayPushToCloudWatchLogs aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de novembro de 2015, 23:41 UTC

- Horário de edição: 11 de novembro de 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppFlowFullAccess

AmazonAppFlowFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon AppFlow e acesso aos serviços da AWS suportados como origem ou destino do fluxo (S3 e Redshift). Também fornece acesso ao KMS para criptografia

### A utilização desta política

Você pode vincular a AmazonAppFlowFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de junho de 2020, 23:30 UTC
- Horário de edição: 28 de fevereiro de 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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



```
{
  "Sid" : "S3ReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3PutBucketPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::appflow-*"
},
{
  "Sid" : "SecretsManagerCreateSecretAccess",
  "Effect" : "Allow",
  "Action" : "secretsmanager:CreateSecret",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:Name" : "appflow!*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "appflow.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "SecretsManagerPutResourcePolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:PutResourcePolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppFlowReadOnlyAccess

AmazonAppFlowReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura aos fluxos do Amazon AppFlow

### A utilização desta política

Você pode vincular a AmazonAppFlowReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 02 de junho de 2020, 23:26 UTC
- Horário de edição: 28 de fevereiro de 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppStreamFullAccess

AmazonAppStreamFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon AppStream por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonAppStreamFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 28 de agosto de 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Resource" : "*"
  },
  {
    "Action" : [
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:RegisterScalableTarget",
      "application-autoscaling:DescribeScheduledActions",
      "application-autoscaling:PutScheduledAction",
      "application-autoscaling>DeleteScheduledAction"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:PutMetricAlarm"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : "iam:ListRoles",
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : "iam:PassRole",

```

```

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

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppStreamPCAAccess

AmazonAppStreamPCAAccess é uma [política gerenciada da AWS](#) que: acesso do Amazon AppStream 2.0 à CA privada de AWS Certificate Manager em contas de clientes para autenticação baseada em certificados

### A utilização desta política

Você pode vincular a AmazonAppStreamPCAAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Hora de criação: 24 de outubro de 2022, 17:05 UTC
- Horário de edição: 24 de outubro de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppStreamReadOnlyAccess

AmazonAppStreamReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura ao Amazon AppStream por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonAppStreamReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 07 de dezembro de 2016, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```



```
    "appstream:List*",
    "appstream:Describe*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAppStreamServiceAccess

AmazonAppStreamServiceAccess é uma [política gerenciada da AWS](#) que: política padrão para a função de serviço Amazon AppStream.

### A utilização desta política

Você pode vincular a AmazonAppStreamServiceAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de novembro de 2016, 04:17 UTC
- Horário de edição: 26 de junho de 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
"Resource" : [  
  "arn:aws:s3:::appstream2-36fb080bb8-*",  
  "arn:aws:s3:::appstream-app-settings-*",  
  "arn:aws:s3:::appstream-logs-*"  
]  
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAthenaFullAccess

AmazonAthenaFullAccess é uma [política gerenciada AWS](#) que: fornecer acesso total ao Amazon Athena e acesso com escopo às dependências necessárias para permitir a consulta, a gravação de resultados e o gerenciamento de dados.

### Utilização desta política

Você pode vincular a AmazonAthenaFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 30 de novembro de 2016, 16:46 UTC
- Horário editado: 03 de janeiro de 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAugmentedAIFullAccess

AmazonAugmentedAIFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso para executar todas as operações dos recursos do Amazon Augmented AI, incluindo FlowDefinitions, HumanTaskUis e HumanLoops. Não permite acesso para criar FlowDefinitions contra a equipe de trabalho pública.

## A utilização desta política

Você pode vincular a AmazonAugmentedAIFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 16:21 UTC
- Horário de edição: 03 de dezembro de 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso para realizar todas as operações no HumanLoops.

### A utilização desta política

Você pode vincular a AmazonAugmentedAIHumanLoopFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 03 de dezembro de 2019, 16:20 UTC
- Horário de edição: 03 de dezembro de 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonAugmentedAIIntegratedAPIAccess

AmazonAugmentedAIIntegratedAPIAccess é uma [política gerenciada da AWS](#) que: fornece acesso para executar todas as operações dos recursos do Amazon Augmented AI, incluindo FlowDefinitions, HumanTaskUis e HumanLoops. Também fornece acesso às operações de serviços que são integradas com o Amazon Augmented AI.

## A utilização desta política

Você pode vincular a AmazonAugmentedAIIntegratedAPIAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de abril de 2020, 20:47 UTC
- Horário de edição: 22 de abril de 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
```

```

    "sagemaker:*HumanTaskUi",
    "sagemaker:*HumanTaskUis"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "sagemaker:WorkteamType" : [
        "private-crowd",
        "vendor-crowd"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "textract:AnalyzeDocument"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rekognition:DetectModerationLabels"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonBedrockFullAccess

AmazonBedrockFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Bedrock, bem como acesso limitado aos serviços relacionados que são exigidos por ele

### Utilização desta política

Você pode vincular a AmazonBedrockFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de dezembro de 2023, 15:47 UTC
- Horário editado: 06 de dezembro de 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```
{
  "Sid" : "BedrockAll",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeKey",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : "arn:*:kms:*:::*"
},
{
  "Sid" : "APIsWithAllResourceAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PassRoleToBedrock",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "bedrock.amazonaws.com"
      ]
    }
  }
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonBedrockReadOnly

AmazonBedrockReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Bedrock

### Utilização desta política

Você pode vincular a AmazonBedrockReadOnly aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de dezembro de 2023, 15:48 UTC
- Horário editado: 06 de dezembro de 2023, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonBraketFullAccess

AmazonBraketFullAccess é uma [política gerenciada da AWS](#) que: Fornece acesso total ao Amazon Braket por meio do AWS Management Console e do SDK. Também fornece acesso a serviços relacionados (por exemplo, S3, registros).

## A utilização desta política

Você pode vincular a AmazonBraketFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de agosto de 2020, 20:12 UTC
- Horário de edição: 19 de abril de 2023, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ]
    }
  ],
}
```

```
    "Resource" : "arn:aws:s3:::amazon-braket-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "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"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicy é uma [política gerenciada da AWS](#) que: concede acesso Serviços da AWS e atributos necessários para executar uma tarefa do Amazon Braket, incluindo S3, Cloudwatch, IAM e Braket

## A utilização desta política

Você pode vincular a AmazonBraketJobsExecutionPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de novembro de 2021, 19:34 UTC
- Horário de edição: 28 de novembro de 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ]
    }
  ],
}
```

```
    "Resource" : "arn:aws:s3:::amazon-braket-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
      "ecr:BatchCheckLayerAvailability"
    ],
    "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetAuthorizationToken"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "braket:CancelJob",
      "braket:CancelQuantumTask",
      "braket:CreateJob",
      "braket:CreateQuantumTask",
      "braket:GetDevice",
      "braket:GetJob",
      "braket:GetQuantumTask",
      "braket:SearchDevices",
      "braket:SearchJobs",
      "braket:SearchQuantumTasks",
      "braket:ListTagsForResource",
      "braket:TagResource",
      "braket:UntagResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/service-role/AmazonBraketJobsExecutionRole*",
    "Condition" : {
```

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



```
    }  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonBraketServiceRolePolicy

AmazonBraketServiceRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon Braket crie e gerencie atributos de AWS em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de agosto de 2020, 17:12 UTC
- Horário de edição: 06 de agosto de 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonChimeFullAccess

AmazonChimeFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Console de administração do Amazon Chime por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonChimeFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de novembro de 2017, 22:15 UTC
- Horário de edição: 14 de dezembro de 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
```

```
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "logs:CreateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:GetLogDelivery",
    "logs:ListLogDeliveries",
    "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy",
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:GetTopicAttributes"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:GetQueueAttributes",
    "sqs:CreateQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
  ]
},
{
```

```
    "Action" : [
      "kinesis:ListStreams"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:DescribeStream"
    ],
    "Resource" : [
      "arn:aws:kinesis:*:*:stream/chime-chat-*",
      "arn:aws:kinesis:*:*:stream/chime-messaging-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetEncryptionConfiguration",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::chime-chat-*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonChimeReadOnly

AmazonChimeReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso total ao Console de administração do Amazon Chime por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonChimeReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de novembro de 2017, 22:04 UTC
- Horário de edição: 14 de dezembro de 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

## Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeSDK

AmazonChimeSDK é uma [política gerenciada da AWS](#) que: fornece acesso às operações do SDK do Amazon Chime

### A utilização desta política

Você pode vincular a AmazonChimeSDK aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de fevereiro de 2020, 21:53 UTC
- Horário de edição: 10 de janeiro de 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime>DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime>DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime>DeleteMediaCapturePipeline",
        "chime>DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy é uma [política AWS gerenciada](#) [que: Política](#) gerenciada para Amazon Chime SDK MediaPipelines Service Linked Role

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de abril de 2022, 22:02 UTC
- Horário editado: 08 de dezembro de 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
```

```
    "Action" : [  
      "chime:GetMeeting",  
      "chime:CreateAttendee",  
      "chime>DeleteAttendee"  
    ],  
    "Resource" : "*"    
  }  
]  
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy é uma [política gerenciada da AWS](#) que: Permite que o Messaging do SDK do Amazon Chime acesse atributos de AWS e habilite a funcionalidade de mensagens

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de março de 2023, 01:43 UTC
- Horário de edição: 03 de março de 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite o acesso aos atributos de AWS usados ou gerenciados pelo Amazon Chime

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de setembro de 2019, 22:25 UTC
- Horário de edição: 30 de setembro de 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime"
      ]
    }
  ]
}
```

```
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "chime.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy é uma [política gerenciada da AWS](#) que: permite que o Amazon Chime acesse o Amazon Transcribe e o Amazon Transcribe Medical em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de agosto de 2021, 21:47 UTC
- Horário de edição: 04 de agosto de 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeUserManagement

AmazonChimeUserManagement é uma [política gerenciada da AWS](#) que: fornece acesso total ao Console de administração do Amazon Chime por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonChimeUserManagement aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de novembro de 2017, 22:17 UTC

- Horário de edição: 18 de fevereiro de 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime: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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy é uma [política gerenciada da AWS](#) que: política gerenciada para a função vinculada ao serviço no Voice Connector do Amazon Chime

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de setembro de 2019, 22:16 UTC
- Horário de edição: 14 de abril de 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
```

```

    "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:ListStreams"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:SendMessage"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "polly:SynthesizeSpeech"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "chime:CreateMediaInsightsPipeline",
    "chime:GetMediaInsightsPipelineConfiguration"
  ]
}

```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess é uma [política gerenciada da AWS](#) que: Fornece acesso total ao serviço do Amazon Cloud Directory.

### A utilização desta política

Você pode vincular a AmazonCloudDirectoryFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de fevereiro de 2017, 00:41 UTC
- Horário de edição: 25 de fevereiro de 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudDirectoryReadOnlyAccess

AmazonCloudDirectoryReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao serviço do Amazon Cloud Directory.

### A utilização desta política

Você pode vincular a AmazonCloudDirectoryReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 28 de fevereiro de 2017, 23:42 UTC
- Horário de edição: 28 de fevereiro de 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonCloudWatchEvidentlyFullAccess

AmazonCloudWatchEvidentlyFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao serviço do Amazon CloudWatch Evidently. Também fornece acesso ao Amazon S3, Amazon SNS, Amazon CloudWatch e outros serviços relacionados.

## A utilização desta política

Você pode vincular a AmazonCloudWatchEvidentlyFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 15:10 UTC
- Horário de edição: 29 de novembro de 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/CloudWatchRUMevidentlyRole-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "arn:aws:s3:::*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:DescribeAlarmHistory",
      "cloudwatch:DescribeAlarmsForMetric",
      "cloudwatch:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms",
      "cloudwatch:TagResource",
      "cloudwatch:UntagResource"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:*"
    ]
  }

```



```
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:LookupEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:Subscribe",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "arn:*:sns:*:*:Evidently-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
    ]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudWatchEvidentlyReadOnlyAccess

AmazonCloudWatchEvidentlyReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao serviço do Amazon CloudWatch Evidently.

### A utilização desta política

Você pode vincular a AmazonCloudWatchEvidentlyReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 15:08 UTC
- Horário de edição: 29 de novembro de 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudWatchEvidentlyServiceRolePolicy

AmazonCloudWatchEvidentlyServiceRolePolicy é uma [política gerenciada da AWS](#) que permite que o serviço do CloudWatch Evidently gerencie os atributos de AWS associados em nome do cliente

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de setembro de 2022, 17:25 UTC
- Horário de edição: 13 de setembro de 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
```

```
"Effect" : "Deny",
"Action" : "appconfig:StartDeployment",
"Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
"Condition" : {
  "StringNotEquals" : {
    "aws:ResourceTag/Owner" : "Evidently"
  }
},
{
  "Effect" : "Allow",
  "Action" : "appconfig:TagResource",
  "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/DeployedBy" : "Evidently"
    }
},
{
  "Effect" : "Allow",
  "Action" : "appconfig:StopDeployment",
  "Resource" : "arn:aws:appconfig:*:*:application/*"
},
{
  "Effect" : "Deny",
  "Action" : "appconfig:StopDeployment",
  "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceTag/DeployedBy" : "Evidently"
    }
},
{
  "Effect" : "Allow",
  "Action" : "appconfig:ListDeployments",
  "Resource" : "arn:aws:appconfig:*:*:application/*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudWatchRUMFullAccess

AmazonCloudWatchRUMFullAccess é uma [política gerenciada da AWS](#) que: concede permissões de acesso total ao serviço Amazon CloudWatch RUM

### A utilização desta política

Você pode vincular a AmazonCloudWatchRUMFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 15:46 UTC
- Horário de edição: 29 de novembro de 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "rum:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/RUM-Monitor*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "cognito-identity.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ]
}

```

```

    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cognito-identity:CreateIdentityPool",
      "cognito-identity:ListIdentityPools",
      "cognito-identity:DescribeIdentityPool",
      "cognito-identity:GetIdentityPoolRoles",
      "cognito-identity:SetIdentityPoolRoles"
    ],
    "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs>DeleteLogGroup",
      "logs:PutRetentionPolicy",
      "logs:CreateLogStream"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:ListLogDeliveries",
      "logs:DescribeResourcePolicies"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
  },
  {

```



```
    "Effect" : "Allow",
    "Action" : [
      "synthetics:describeCanaries",
      "synthetics:describeCanariesLastRun"
    ],
    "Resource" : "arn:aws:synthetics:*:*:canary:*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess é uma [política gerenciada da AWS](#) que: concede permissões de somente leitura ao serviço Amazon CloudWatch RUM

### A utilização desta política

Você pode vincular a AmazonCloudWatchRUMReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 15:43 UTC
- Horário de edição: 28 de outubro de 2022, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonCloudWatchRUMServiceRolePolicy

AmazonCloudWatchRUMServiceRolePolicy é uma [política gerenciada da AWS](#) que: concede permissão ao Amazon CloudWatch RUM Service para publicar dados de monitoramento em outros serviços de AWS relevantes

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de novembro de 2021, 23:17 UTC
- Horário de edição: 22 de fevereiro de 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "cloudwatch:namespace" : [
          "RUM/CustomMetrics/*",
          "AWS/RUM"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeCatalystFullAccess

AmazonCodeCatalystFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon CodeCatalyst

### A utilização desta política

Você pode vincular a AmazonCodeCatalystFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de abril de 2023, 16:50 UTC

- Horário de edição: 20 de abril de 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeCatalystReadOnlyAccess

AmazonCodeCatalystReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao Amazon CodeCatalyst

### A utilização desta política

Você pode vincular a AmazonCodeCatalystReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de abril de 2023, 16:49 UTC
- Horário de edição: 20 de abril de 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeCatalystSupportAccess

AmazonCodeCatalystSupportAccess é uma [política gerenciada da AWS](#) que: permite que o Amazon CodeCatalyst crie, atualize e resolva casos de AWS Support em seu nome.

### A utilização desta política

Você pode vincular a AmazonCodeCatalystSupportAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de abril de 2023, 12:34 UTC
- Horário de edição: 20 de abril de 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)



- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruProfilerAgentAccess

AmazonCodeGuruProfilerAgentAccess é uma [política gerenciada da AWS](#) que: fornece o acesso exigido pelo atendente do Amazon CodeGuru Profiler.

### A utilização desta política

Você pode vincular a AmazonCodeGuruProfilerAgentAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de fevereiro de 2021, 22:11 UTC
- Horário de edição: 05 de maio de 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "codeguru-profiler:ConfigureAgent",
      "codeguru-profiler>CreateProfilingGroup",
      "codeguru-profiler:PostAgentProfile"
    ],
    "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruProfilerFullAccess

AmazonCodeGuruProfilerFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon CodeGuru Profiler.

### A utilização desta política

Você pode vincular a AmazonCodeGuruProfilerFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 10:13 UTC
- Horário de edição: 15 de julho de 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruProfilerReadOnlyAccess

AmazonCodeGuruProfilerReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao Amazon CodeGuru Profiler.

### A utilização desta política

Você pode vincular a AmazonCodeGuruProfilerReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 10:30 UTC
- Horário de edição: 27 de junho de 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
```

```
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruReviewerFullAccess

AmazonCodeGuruReviewerFullAccess é uma [política gerenciada da AWS](#) que: concede acesso total ao Amazon CodeGuru Reviewer e acesso definido às dependências necessárias.

### A utilização desta política

Você pode vincular a AmazonCodeGuruReviewerFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 08:33 UTC
- Horário de edição: 29 de agosto de 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
```

```
"Action" : [
  "codecommit:ListRepositories"
],
"Resource" : "*"
},
{
  "Sid" : "CodeCommitTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:TagResource",
    "codecommit:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "codeguru-reviewer"
    }
  }
},
{
  "Sid" : "CodeConnectTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:TagResource",
    "codestar-connections:UntagResource",
    "codestar-connections:ListTagsForResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "codeguru-reviewer"
    }
  }
},
{
  "Sid" : "CodeConnectManagedRules",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codestar-connections:ListConnections",
    "codestar-connections:PassConnection"
  ],
  "Resource" : "*",
  "Condition" : {
```

```
    "ForAllValues:StringEquals" : {
      "codestar-connections:ProviderAction" : [
        "ListRepositories",
        "ListOwners"
      ]
    }
  },
  {
    "Sid" : "CloudWatchEventsManagedRules",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule",
      "events:PutTargets",
      "events>DeleteRule",
      "events:RemoveTargets"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruReviewerReadOnlyAccess

AmazonCodeGuruReviewerReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao Amazon CodeGuru Reviewer.



## A utilização desta política

Você pode vincular a `AmazonCodeGuruReviewerReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 08:48 UTC
- Horário de edição: 29 de agosto de 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy é uma [política gerenciada da AWS](#) que: é necessária uma função vinculada ao serviço para que o Amazon CodeGuru Reviewer acesse recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de dezembro de 2019, 05:31 UTC
- Horário de edição: 27 de novembro de 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",

```

```
        "ListPullRequestComments",
        "ListPullRequestCommits",
        "ListCommitFiles",
        "ListBranchCommits",
        "CreatePullRequestDiffComment",
        "GitPull"
    ]
},
"Null" : {
    "aws:ResourceTag/codeguru-reviewer" : "false"
}
},
{
    "Sid" : "CloudWatchEventsResourceCleanup",
    "Effect" : "Allow",
    "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowGuruS3GetObject",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
        "arn:aws:s3:::codeguru-reviewer-*/*"
    ]
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruSecurityFullAccess

AmazonCodeGuruSecurityFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon CodeGuru Security.

### A utilização desta política

Você pode vincular a AmazonCodeGuruSecurityFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2023, 21:03 UTC
- Horário de edição: 09 de maio de 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCodeGuruSecurityScanAccess

AmazonCodeGuruSecurityScanAccess é uma [política gerenciada da AWS](#) que: fornece o acesso necessário para trabalhar com as verificações do Amazon CodeGuru Security.

### A utilização desta política

Você pode vincular a AmazonCodeGuruSecurityScanAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2023, 20:54 UTC
- Horário de edição: 09 de maio de 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoDeveloperAuthenticatedIdentities

AmazonCognitoDeveloperAuthenticatedIdentities é uma [política gerenciada da AWS](#) que: fornece acesso às APIs do Amazon Cognito para dar suporte às identidades autenticadas do desenvolvedor a partir de seu backend de autenticação.

## A utilização desta política

Você pode vincular a `AmazonCognitoDeveloperAuthenticatedIdentities` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de março de 2015, 17:22 UTC
- Horário de edição: 24 de março de 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoIdpEmailServiceRolePolicy

AmazonCognitoIdpEmailServiceRolePolicy é uma [política gerenciada da AWS](#) que: Permite que o serviço de grupos de usuários do Amazon Cognito use suas identidades SES para envio de e-mails

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de março de 2019, 21:32 UTC
- Horário de edição: 21 de março de 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoIdpServiceRolePolicy

AmazonCognitoIdpServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite o acesso aos atributos de Serviços da AWS usados ou gerenciados pelos grupos de usuários do Amazon Cognito

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de junho de 2020, 22:30 UTC
- Horário de edição: 26 de junho de 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonCognitoPowerUser

AmazonCognitoPowerUser é uma [política gerenciada da AWS](#) que: fornece acesso administrativo aos atributos existentes do Amazon Cognito. Você precisará de privilégios de Conta da AWS administrador para criar novos tributos no Cognito.

## A utilização desta política

Você pode vincular a AmazonCognitoPowerUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de março de 2015, 17:14 UTC
- Horário de edição: 01 de junho de 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
```

```

    "iam:GetSAMLProvider",
    "kinesis:ListStreams",
    "lambda:GetPolicy",
    "lambda:ListFunctions",
    "sns:GetSMSSandboxAccountStatus",
    "sns:ListPlatformApplications",
    "ses:ListIdentities",
    "ses:GetIdentityVerificationAttributes",
    "mobiletargeting:GetApps",
    "acm:ListCertificates"
  ],
  "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*"
  ]
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoReadOnly

AmazonCognitoReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura aos atributos do Amazon Cognito.

### A utilização desta política

Você pode vincular a AmazonCognitoReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de março de 2015, 17:06 UTC
- Horário de edição: 01 de agosto de 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "cognito-identity:Describe*",
    "cognito-identity:Get*",
    "cognito-identity:List*",
    "cognito-idp:Describe*",
    "cognito-idp:AdminGet*",
    "cognito-idp:AdminList*",
    "cognito-idp:List*",
    "cognito-idp:Get*",
    "cognito-sync:Describe*",
    "cognito-sync:Get*",
    "cognito-sync:List*",
    "iam:ListOpenIdConnectProviders",
    "iam:ListRoles",
    "sns:ListPlatformApplications"
  ],
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoUnAuthedIdentitiesSessionPolicy

AmazonCognitoUnAuthedIdentitiesSessionPolicy é uma [política gerenciada da AWS](#) que: essa política define o conjunto de permissões permitidas para identidades não autenticadas para o Cognito Identity Pools. Esta política não se destina a ser usada como uma política de permissão independente. Ela é utilizada como uma barreira de proteção contra políticas excessivamente permissivas associadas a funções em um banco de identidades. Não vincule esta política a qualquer função, pois o Serviço de Identidade Cognito a incorporará automaticamente como uma política com

escopo reduzido durante a criação de credenciais. Os privilégios para acessar temporariamente outros atributos de AWS por meio do fluxo aprimorado serão agora definidos pela interseção entre a função associada à identidade do usuário não autenticado fornecida por um serviço e os privilégios fornecidos por essa política gerenciada de propriedade do Cognito.

## A utilização desta política

Você pode vincular a `AmazonCognitoUnAuthedIdentitiesSessionPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de julho de 2023, 23:04 UTC
- Horário de edição: 19 de julho de 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
```



```
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonCognitoUnauthenticatedIdentities

AmazonCognitoUnauthenticatedIdentities é uma [política gerenciada da AWS](#) que: essa política define o conjunto de permissões permitidas para identidades não autenticadas para o Cognito Identity Pools. Não vincule esta política a qualquer função, pois o Serviço de Identidade Cognito a incorporará automaticamente como uma política com escopo reduzido durante a criação de credenciais. Os privilégios para acessar temporariamente outros atributos de AWS por meio do fluxo aprimorado serão agora definidos pela interseção entre a função associada à identidade do usuário não autenticado fornecida por um serviço e os privilégios fornecidos por essa política gerenciada de propriedade do Cognito.

### A utilização desta política

Você pode vincular a AmazonCognitoUnauthenticatedIdentities aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 01 de fevereiro de 2023, 22:36 UTC
- Horário de edição: 01 de fevereiro de 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnect\_FullAccess

AmazonConnect\_FullAccess é uma [política gerenciada da AWS](#) que: O objetivo dessa política é conceder permissões aos usuários do AWS Connect que precisam usar os atributos do Connect.

Esta política fornece acesso total aos atributos do AWS Connect por meio do Connect Console e de APIs públicas

## A utilização desta política

Você pode vincular a `AmazonConnect_FullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de novembro de 2020, 19:54 UTC
- Horário de edição: 07 de março de 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds>DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
```

```
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lex:GetBots",
    "lex:ListBots",
    "lex:ListBotAliases",
    "logs:CreateLogGroup",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "lambda:ListFunctions",
    "ds:CheckAlias",
    "profile:ListAccountIntegrations",
    "profile:GetDomain",
    "profile:ListDomains",
    "profile:GetProfileObjectType",
    "profile:ListProfileObjectTypeTemplates"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "profile:AddProfileKey",
    "profile:CreateDomain",
    "profile:CreateProfile",
    "profile>DeleteDomain",
    "profile>DeleteIntegration",
    "profile>DeleteProfile",
    "profile>DeleteProfileKey",
    "profile>DeleteProfileObject",
    "profile>DeleteProfileObjectType",
    "profile:GetIntegration",
    "profile:GetMatches",
    "profile:GetProfileObjectType",
    "profile:ListIntegrations",
    "profile:ListProfileObjects",
    "profile:ListProfileObjectTypes",
    "profile:ListTagsForResource",
    "profile:MergeProfiles",
    "profile:PutIntegration",
    "profile:PutProfileObject",
    "profile:PutProfileObjectType",
    "profile:SearchProfiles",
    "profile:TagResource",
```

```

        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
    ],
    "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
    ],
    "Resource" : "arn:aws:s3:::amazon-connect-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "arn:aws:servicequotas:*:*:connect/*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "connect.amazonaws.com"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : "iam>DeleteServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/profile.amazonaws.com/*",
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "profile.amazonaws.com"
        }
    }
}

```

```
    }  
  }  
} ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnectCampaignsServiceLinkedRolePolicy

AmazonConnectCampaignsServiceLinkedRolePolicy é uma [política gerenciada pela AWS](#) que: política para a função vinculada ao serviço Amazon Connect Campaigns

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de setembro de 2021, 20:54 UTC
- Hora da edição: 08 de novembro de 2023, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnectReadOnlyAccess

AmazonConnectReadOnlyAccess é uma [política gerenciada da AWS](#) que: Concede permissão para visualizar as instâncias do Amazon Connect em seu Conta da AWS.

## A utilização desta política

Você pode vincular a `AmazonConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 17 de outubro de 2018, 21:00 UTC
- Horário de edição: 06 de novembro de 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "connect:GetFederationTokens",
      "Resource" : "*"
    }
  ]
}
```



```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnectServiceLinkedRolePolicy

AmazonConnectServiceLinkedRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon Connect crie e gerencie atributos de AWS em seu nome

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de setembro de 2018, 00:21 UTC
- Horário editado: 28 de novembro de 2023, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",

```

```
    "s3:GetBucketAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::amazon-connect-*"
  ]
},
{
  "Sid" : "AllowConnectLogGroupAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
  ]
},
{
  "Sid" : "AllowListLexBotAccess",
  "Effect" : "Allow",
  "Action" : [
    "lex:ListBots",
    "lex:ListBotAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowCustomerProfilesForConnectDomain",
  "Effect" : "Allow",
  "Action" : [
    "profile:SearchProfiles",
    "profile:CreateProfile",
    "profile:UpdateProfile",
    "profile:AddProfileKey",
    "profile:ListProfileObjectTypes",
    "profile:ListCalculatedAttributeDefinitions",
    "profile:ListCalculatedAttributesForProfile",
    "profile:GetDomain",
    "profile:ListIntegrations"
  ],
  "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"
  ],
  "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}"
    }
  }
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon Connect crie e gerencie atributos de AWS em seu nome

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de outubro de 2023, 22:38 UTC
- Horário editado: 27 de outubro de 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonConnectVoiceIDFullAccess

AmazonConnectVoiceIDFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Connect Voice ID

### A utilização desta política

Você pode vincular a AmazonConnectVoiceIDFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 26 de setembro de 2021, 19:04 UTC
- Horário de criação: 26 de setembro de 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZoneDomainExecutionRolePolicy

AmazonDataZoneDomainExecutionRolePolicy é uma [política AWS gerenciada](#) que: Política padrão para a função DataZone de DomainExecutionRole serviço da Amazon. Essa função é

usada pela Amazon DataZone para catalogar, descobrir, controlar, compartilhar e analisar dados no DataZone domínio da Amazon.

## Utilização desta política

Você pode vincular a `AmazonDataZoneDomainExecutionRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 27 de setembro de 2023, 21:55 UTC
- Horário editado: 12 de março de 2024, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datzone:AcceptPredictions",
        "datzone:AcceptSubscriptionRequest",
        "datzone:CancelSubscription",
        "datzone:CreateAsset",
        "datzone:CreateAssetRevision",
        "datzone:CreateAssetType",
        "datzone: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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonDataZoneEnvironmentRolePermissionsBoundary

AmazonDataZoneEnvironmentRolePermissionsBoundary é uma [política AWS gerenciada](#) que: DataZone A Amazon cria funções do IAM para ambientes realizarem ações de análise de dados e usa essa política ao criar essas funções para definir o limite de suas permissões.

### Utilização desta política

Você pode vincular a AmazonDataZoneEnvironmentRolePermissionsBoundary aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 11 de setembro de 2023, 23:38 UTC
- Horário editado: 17 de novembro de 2023, 23:29 UTC

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

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
```

```
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetWorkflows",
"glue:BatchStopJobRun",
"glue:BatchUpdatePartition",
"glue:CreateBlueprint",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteBlueprint",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeleteConnection",
"glue>DeleteCrawler",
"glue>DeleteJob",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
"glue>DeleteTable",
"glue>DeleteTableVersion",
"glue>DeleteWorkflow",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:PutWorkflowRunProperties",
"glue:ResetJobBookmark",
"glue:ResumeWorkflowRun",
"glue:SearchTables",
"glue:StartBlueprintRun",
"glue:StartCrawler",
```



```

    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:StartWorkflowRun",
    "glue:StopCrawler",
    "glue:StopCrawlerSchedule",
    "glue:StopWorkflowRun",
    "glue:UpdateBlueprint",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:UpdateConnection",
    "glue:UpdateCrawler",
    "glue:UpdateCrawlerSchedule",
    "glue:UpdateDatabase",
    "glue:UpdateJob",
    "glue:UpdatePartition",
    "glue:UpdateTable",
    "glue:UpdateWorkflow"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "PassRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/datazone*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "glue.amazonaws.com"
    }
  }
},
{
  "Sid" : "SameAccountKmsOperations",
  "Effect" : "Allow",
  "Action" : [

```

```

    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "KmsOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:Verify",
    "kms:Sign"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AnalyticsOperations",
  "Effect" : "Allow",
  "Action" : [
    "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" : [
    "*"
  ]
}
]

```

}

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZoneFullAccess

AmazonDataZoneFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à Amazon DataZone por meio de acesso limitado e acesso aos serviços relacionados que são exigidos por ela. AWS Management Console

### Utilização desta política

Você pode vincular a AmazonDataZoneFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2023, 20:06 UTC
- Horário editado: 12 de março de 2024, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2: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" : "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_*"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonDataZoneFullUserAccess

`AmazonDataZoneFullUserAccess` é uma [política AWS gerenciada](#) que: fornece acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas.

### Utilização desta política

Você pode vincular a `AmazonDataZoneFullUserAccess` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2023, 21:06 UTC
- Horário editado: 12 de março de 2024, 23:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

### Versão da política

Versão da política: v5 (padrão)



A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsWithUser",
        "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" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AmazonDataZoneGlueManageAccessRolePolicy

AmazonDataZoneGlueManageAccessRolePolicy é uma [política AWS gerenciada](#) que: A política concede permissões para permitir que DataZone a Amazon habilite concessões de publicação e acesso a dados.

## Utilização desta política

Você pode vincular a AmazonDataZoneGlueManageAccessRolePolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 22 de setembro de 2023, 20:21 UTC
- Horário editado: 14 de dezembro de 2023, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy é uma [política gerenciada da AWS](#) que: fornece acesso total às APIs do Amazon DataZone

### A utilização desta política

Você pode vincular a AmazonDataZonePortalFullAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de março de 2023, 18:24 UTC
- Horário editado: 26 de março de 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total à versão antecipada do Amazon DataZone por meio do AWS Management Console. Também fornece acesso seletivo a outros serviços relacionados.

## A utilização desta política

Você pode vincular a AmazonDataZonePreviewConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de março de 2023, 15:16 UTC
- Horário editado: 13 de julho de 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",

```

```

    "sso:DescribeRegisteredRegions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateConnection"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:connection/AmazonDataZone-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetPolicy",
  "Resource" : [
    "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-AmazonDataZoneBootstrapRole",
    "arn:aws:iam:*:*:policy/service-role/AmazonDataZoneServicePolicy-AmazonDataZoneServiceRole"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam:*:*:role/AmazonDataZoneServiceRole*",
    "arn:aws:iam:*:*:role/service-role/AmazonDataZoneServiceRole*",
    "arn:aws:iam:*:*:role/AmazonDataZoneBootstrapRole*",
    "arn:aws:iam:*:*:role/service-role/AmazonDataZoneBootstrapRole",
    "arn:aws:iam:*:*:role/AmazonDataZoneDomainExecutionRole",
    "arn:aws:iam:*:*:role/service-role/AmazonDataZoneDomainExecutionRole"
  ]
},

```

```
    "Condition" : {
      "StringEquals" : {
        "iam:passedToService" : "datazonecontrol.amazonaws.com"
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary é uma [política gerenciada da AWS](#) que: O Amazon DataZone cria funções do IAM que são usadas para implantar projetos de análise de dados. O DataZone usa essa política ao criar essas funções para definir o limite de suas permissões.

### A utilização desta política

Você pode vincular a AmazonDataZoneProjectDeploymentPermissionsBoundary aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de março de 2023, 02:54 UTC
- Horário editado: 04 de abril de 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
```

```

    "kms:TagResource",
    "athena:CreateWorkGroup",
    "athena:TagResource",
    "iam:TagRole",
    "iam:TagPolicy",
    "logs:CreateLogGroup",
    "logs:TagLogGroup",
    "ssm:AddTagsToResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : "datazone:*"
    },
    "StringLike" : {
      "aws:ResourceTag/datazone:projectId" : "proj-*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "athena>DeleteWorkGroup",
    "kms:ScheduleKeyDeletion",
    "kms:DescribeKey",
    "kms:EnableKeyRotation",
    "kms:DisableKeyRotation",
    "kms:GenerateDataKey",
    "kms:Encrypt",
    "kms:Decrypt",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/datazone:projectId" : "proj-*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ]
}

```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "datazone:projectId"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeletePolicy",
      "s3:DeleteBucket"
    ],
    "Resource" : [
      "arn:aws:iam::*:policy/datazone*",
      "arn:aws:s3:::datazone*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter*",
      "ssm:PutParameter",
      "ssm:DeleteParameter"
    ],
    "Resource" : [
      "arn:aws:ssm::*:parameter/*datazone*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:GetPolicy",
      "iam:GetRolePolicy",
      "iam:CreatePolicy",
      "iam:ListPolicyVersions",
      "lakeformation:RegisterResource",
      "lakeformation:DeregisterResource",
      "lakeformation:GrantPermissions",
      "lakeformation:PutDataLakeSettings",
      "lakeformation:GetDataLakeSettings",
      "lakeformation:RevokePermissions",
```

```

    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabases",
    "glue:GetDatabase",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/*datazone*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock",
    "s3>DeleteBucketPolicy",
    "s3>CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketAcl",
    "s3:PutBucketVersioning",
    "s3:PutBucketTagging",
    "s3:PutBucketLogging",
    "s3:GetObject*",
    "s3:GetBucket*",
    "s3:List*",
    "s3:GetEncryptionConfiguration",
    "s3>DeleteObject*",
    "s3:PutObject*",
    "s3:Abort*"
  ],
  "Resource" : "arn:aws:s3::*:datazone*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}

```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "athena:Get*",
      "athena:List*",
      "ec2:CreateSecurityGroup",
      "ec2:RevokeSecurityGroupEgress",
      "ec2>DeleteSecurityGroup",
      "ec2:Describe*",
      "ec2:Get*",
      "ec2:List*",
      "logs:PutRetentionPolicy",
      "logs:DescribeLogGroups",
      "logs>DeleteLogGroup",
      "logs>DeleteRetentionPolicy"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:PutKeyPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
"Condition" : {
  "StringLike" : {
    "ec2:VpceServiceName" : [
      "com.amazonaws.*.logs",
      "com.amazonaws.*.s3",
      "com.amazonaws.*.glue",
      "com.amazonaws.*.athena"
    ]
  }
},
{
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:GetTemplate",
    "cloudformation:DescribeChangeSet",
    "cloudformation:CreateChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation:CreateStack",
    "cloudformation:UpdateStack",
    "cloudformation>DeleteStack",
    "cloudformation:TagResource",
    "cloudformation:GetTemplateSummary"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "s3:GetObject*",
    "s3:GetBucket*",
    "s3:List*",
    "s3:GetEncryptionConfiguration",
    "s3>DeleteObject*",
    "s3:PutObject*",
    "s3:Abort*",
    "s3>DeleteBucket"
  ],
  "NotResource" : [
```

```
    "arn:aws:s3::*datazone*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "kms:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Effect" : "Deny",
  "NotAction" : [
    "ssm:PutParameter",
    "ssm>DeleteParameter",
    "ssm:AddTagsToResource",
    "ssm:GetParameters",
    "ssm:GetParameter",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock",
    "s3>DeleteBucketPolicy",
    "s3>CreateBucket",
    "s3:PutBucketAcl",
    "s3:PutBucketPolicy",
    "s3:PutBucketVersioning",
    "s3:PutBucketTagging",
    "s3:ListBucket",
    "s3:PutBucketLogging",
    "s3>DeleteBucket",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetPolicy",
    "iam>CreatePolicy",
    "iam:ListPolicyVersions",
    "iam>DeletePolicy",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:GetTemplate",
    "cloudformation:DescribeChangeSet",
```

```
"cloudformation:CreateChangeSet",
"cloudformation:ExecuteChangeSet",
"cloudformation>DeleteChangeSet",
"cloudformation:TagResource",
"cloudformation:CreateStack",
"cloudformation:UpdateStack",
"cloudformation>DeleteStack",
"cloudformation:GetTemplateSummary",
"athena:*",
"kms:*",
"glue:CreateDatabase",
"glue>DeleteDatabase",
"glue:GetDatabases",
"glue:GetDatabase",
"lambda:*",
"ec2:*",
"logs:*",
"servicecatalog:CreateApplication",
"servicecatalog>DeleteApplication",
"servicecatalog:GetApplication",
"lakeformation:RegisterResource",
"lakeformation:DeregisterResource",
"lakeformation:GrantPermissions",
"lakeformation:PutDataLakeSettings",
"lakeformation:RevokePermissions",
"lakeformation:GetDataLakeSettings",
"lakeformation:ListPermissions",
"iam:CreateRole",
"iam>DeleteRole",
"iam:DetachRolePolicy",
"iam>DeleteRolePolicy",
"iam:AttachRolePolicy",
"iam:PutRolePolicy",
"iam:UntagRole",
"iam:PassRole",
"iam:TagRole",
"s3:GetBucket*",
"s3:GetObject*",
"s3:Abort*",
"s3:GetEncryptionConfiguration",
"s3:PutObject*"
],
"Resource" : [
  "*"
]
```

```
    ]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZoneProjectRolePermissionsBoundary

AmazonDataZoneProjectRolePermissionsBoundary é uma [política gerenciada da AWS](#) que: o Amazon DataZone cria funções do IAM para ambientes realizarem ações de análise de dados e usa essa política ao criar essas funções para definir o limite de suas permissões.

### A utilização desta política

Você pode vincular a AmazonDataZoneProjectRolePermissionsBoundary aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de março de 2023, 02:51 UTC
- Horário editado: 21 de março de 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:Describe*",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "logs:*",
      "athena:TerminateSession",
      "athena:CreatePreparedStatement",
      "athena:StopCalculationExecution",
      "athena:StartQueryExecution",
      "athena:UpdatePreparedStatement",
      "athena:BatchGet*",
      "athena:List*",
      "athena:UpdateNotebook",
      "athena>DeleteNotebook",
      "athena>DeletePreparedStatement",
      "athena:UpdateNotebookMetadata",
      "athena>DeleteNamedQuery",
      "athena:Get*",
      "athena:UpdateNamedQuery",
      "athena:CreateNamedQuery",
      "athena:ExportNotebook",
      "athena:StopQueryExecution",
      "athena:StartCalculationExecution",
      "athena:StartSession",
      "athena:CreatePresignedNotebookUrl",
      "athena:CreateNotebook",
      "athena:ImportNotebook",
      "organizations:DescribeOrganization",
      "organizations:DescribeAccount",
      "lakeformation:GetDataAccess",
      "lakeformation:BatchGrantPermissions",
      "lakeformation:GrantPermissions",
      "lakeformation:GetDataLakeSettings",
      "lakeformation:PutDataLakeSettings",
      "lakeformation:BatchRevokePermissions",
      "lakeformation:GetResourceLFTags",
      "lakeformation:ListPermissions",
```

```
    "ram:CreateResourceShare",
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare",
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare",
    "ram:AcceptResourceShareInvitation",
    "ram:Get*",
    "ram:List*",
    "redshift:DescribeClusters",
    "redshift:JoinGroup",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift-data:*",
    "redshift:AuthorizeDataShare",
    "redshift:DescribeDataShares",
    "redshift:AssociateDataShareConsumer",
    "tag:GetResources",
    "iam:ListRoles",
    "iam:ListUsers",
    "iam:ListGroups",
    "iam:ListRolePolicies",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "glue:CreateTable",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue:CreatePartitionIndex",
    "glue:CreateDataQualityRuleset",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "glue:CreateWorkflow",
    "sqlworkbench:*",
    "datazone:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ]
},
```



```
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:List*",
    "kms:Get*",
    "kms:Describe*",
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Verify",
    "kms:Sign",
    "kms:GenerateDataKey",
    "glue:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/datazone:projectId" : "false"
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/datazone*"
  ]
}
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
"glue:BatchGet*",
"glue:SearchTables",
"glue:List*",
"glue:Get*",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue>DeleteTable",
"glue:BatchDeleteTable",
"glue:UpdateTable",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:PutResourcePolicy",
"glue:BatchUpdatePartition",
"glue>DeleteTableVersion",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartitionIndex",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:BatchDeleteTableVersion",
"glue:UpdatePartition",
"glue:NotifyEvent",
"glue>DeleteResourcePolicy"
],
"Resource" : "*"
},
{
  "Effect" : "Deny",
  "NotAction" : [
    "s3:List*",
    "s3:Get*",
    "s3:Describe*",
    "s3>DeleteObjectVersion",
    "s3:RestoreObject",
    "s3:ReplicateObject",
    "s3:PutObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutObjectRetention",
    "s3>DeleteObject",
    "kms:List*",
    "kms:Get*",
    "kms:Describe*",
```

```
"kms:Decrypt",
"kms:Encrypt",
"kms:ReEncrypt*",
"kms:Verify",
"kms:Sign",
"kms:GenerateDataKey",
"ec2:Describe*",
"ec2:CreateNetworkInterface",
"ec2>DeleteNetworkInterface",
"ec2:CreateTags",
"ec2>DeleteTags",
"logs:*",
"athena:*",
"glue:BatchGet*",
"glue:Get*",
"glue:SearchTables",
"glue:List*",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue:CreateTable",
"glue>DeleteTable",
"glue:BatchDeleteTable",
"glue:UpdateTable",
"glue:BatchCreatePartition",
"glue:CreatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:PutResourcePolicy",
"glue:CreatePartitionIndex",
"glue:BatchUpdatePartition",
"glue>DeleteTableVersion",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartitionIndex",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:BatchDeleteTableVersion",
"glue:UpdatePartition",
"glue:NotifyEvent",
"glue:StartBlueprintRun",
"glue:PutWorkflowRunProperties",
"glue:StopCrawler",
"glue>DeleteJob",
"glue>DeleteWorkflow",
```

```
"glue:UpdateCrawler",
"glue>DeleteBlueprint",
"glue:UpdateWorkflow",
"glue:StartCrawler",
"glue:ResetJobBookmark",
"glue:UpdateJob",
"glue:StartWorkflowRun",
"glue:StopCrawlerSchedule",
"glue:ResumeWorkflowRun",
"glue>DeleteCrawler",
"glue:UpdateBlueprint",
"glue:BatchStopJobRun",
"glue:StopWorkflowRun",
"glue:UpdateCrawlerSchedule",
"glue>DeleteConnection",
"glue:UpdateConnection",
"glue:BatchDeleteConnection",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue>CreateWorkflow",
"glue:*DataQuality*",
"glue>CreateBlueprint",
"glue>CreateJob",
"glue>CreateConnection",
"glue>CreateCrawler",
"glue>DeleteResourcePolicy",
"organizations:DescribeOrganization",
"organizations:DescribeAccount",
"lakeformation:GetDataAccess",
"lakeformation:BatchGrantPermissions",
"lakeformation:GrantPermissions",
"lakeformation:GetDataLakeSettings",
"lakeformation:PutDataLakeSettings",
"lakeformation:BatchRevokePermissions",
"lakeformation:GetResourceLFTags",
"lakeformation:ListPermissions",
"ram:*",
"redshift:*",
"redshift-data:*",
"tag:GetResources",
"iam:List*",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:PassRole",
```

```
    "sqlworkbench:*",
    "datazone:*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicy é uma [política AWS gerenciada](#) que: DataZone A Amazon é um serviço de gerenciamento de dados que permite catalogar, descobrir, controlar, compartilhar e analisar seus dados. Com a Amazon DataZone, você pode compartilhar e acessar seus dados entre contas e regiões suportadas. A Amazon DataZone simplifica sua experiência em vários AWS serviços, incluindo, mas não se limitando a, Amazon Redshift, Amazon Athena, AWS Glue e Lake Formation. AWS

### Utilização desta política

Você pode vincular a AmazonDataZoneRedshiftGlueProvisioningPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 22 de setembro de 2023, 20:19 UTC
- Horário editado: 12 de março de 2024, 16:44 UTC

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

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
    }
  ]
}
```

```

"Resource" : [
  "arn:aws:iam::*:role/datazone*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com"
    ],
    "aws:CalledViaFirst" : [
      "cloudformation.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteRole",
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/datazone*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
},
{
  "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:TagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation::*:stack/DataZone*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : "AmazonDataZoneEnvironment"
    }
  }
}
}

```

```
    },
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
  ]
},
{
  "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
  "Effect" : "Allow",
  "Action" : [
    "lakeformation:GetDataLakeSettings",
    "lakeformation:PutDataLakeSettings",
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
```



```
    "lakeformation:ListResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:DeleteDatabase"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena:DeleteWorkGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
  "Effect" : "Allow",
```

```

    "Action" : [
      "athena:CreateWorkGroup",
      "athena:TagResource",
      "iam:TagRole",
      "iam:TagPolicy",
      "logs:TagLogGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "AmazonDataZoneEnvironment"
      },
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      },
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs>DeleteLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
    "Condition" : {
      "ForAnyValue:StringLike" : {
        "aws:TagKeys" : "AmazonDataZoneEnvironment"
      },
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      },
      "StringEquals" : {
        "aws:CalledViaFirst" : [
          "cloudformation.amazonaws.com"
        ]
      }
    }
  }
},

```

```
{
  "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
  "Action" : [
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
  "Effect" : "Allow",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeletePolicy",
    "iam:CreatePolicy",
    "iam:GetPolicy",
    "iam:ListPolicyVersions"
  ],
  "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*"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonDataZoneRedshiftManageAccessRolePolicy

AmazonDataZoneRedshiftManageAccessRolePolicy é uma [política AWS gerenciada](#) que: Essa política concede à Amazon DataZone permissões para publicar dados do Amazon Redshift no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do Amazon Redshift ou do Amazon Redshift Serverless no catálogo.

### Utilização desta política

Você pode vincular a AmazonDataZoneRedshiftManageAccessRolePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 22 de setembro de 2023, 20:15 UTC
- Horário editado: 16 de novembro de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```

"Effect" : "Allow",
"Action" : [
  "redshift-data:BatchExecuteStatement",
  "redshift-data:DescribeTable",
  "redshift-data:ExecuteStatement",
  "redshift-data>ListTables",
  "redshift-data>ListSchemas",
  "redshift-data>ListDatabases"
],
"Resource" : [
  "arn:aws:redshift-serverless:*:*:workgroup/*",
  "arn:aws:redshift:*:*:cluster:*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "listSecretsPermission",
  "Effect" : "Allow",
  "Action" : "secretsmanager:ListSecrets",
  "Resource" : "*"
},
{
  "Sid" : "getWorkgroupPermission",
  "Effect" : "Allow",
  "Action" : "redshift-serverless:GetWorkgroup",
  "Resource" : [
    "arn:aws:redshift-serverless:*:*:workgroup/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "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*"
  }
]
}
```



## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDetectiveFullAccess

AmazonDetectiveFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao serviço Amazon Detective e acesso definido às dependências da interface do usuário do console

### A utilização desta política

Você pode vincular a AmazonDetectiveFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 30 de abril de 2020, 17:57 UTC
- Horário editado: 17 de maio de 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "detective:*",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "guardduty:ArchiveFindings"
    ],
    "Resource" : "arn:aws:guardduty:*:*:detector/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "guardduty:GetFindings",
      "guardduty:ListDetectors"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "securityHub:GetFindings"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonDetectiveInvestigatorAccess

AmazonDetectiveInvestigatorAccess é uma [política gerenciada pela AWS](#) que: fornece acesso investigativo ao serviço Amazon Detective e acesso definido às dependências da interface do usuário do console. Esta política concede permissão para entrar em Detective para fins de investigação e acesso de gravação limitado ao GuardDuty.

## Utilização desta política

Você pode vincular a AmazonDetectiveInvestigatorAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 17 de janeiro de 2023, 15:24 UTC
- Horário editado: 27 de novembro de 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",

```

```
    "detective:GetFreeTrialEligibility",
    "detective:GetGraphIngestState",
    "detective:GetMembers",
    "detective:GetPricingInformation",
    "detective:GetUsageInformation",
    "detective:ListDatasourcePackages",
    "detective:ListGraphs",
    "detective:ListHighDegreeEntities",
    "detective:ListInvitations",
    "detective:ListMembers",
    "detective:ListOrganizationAdminAccount",
    "detective:ListTagsForResource",
    "detective:SearchGraph",
    "detective:StartInvestigation",
    "detective:GetInvestigation",
    "detective:ListInvestigations",
    "detective:UpdateInvestigationState",
    "detective:ListIndicators",
    "detective:InvokeAssistant"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GuardDutyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "guardduty:ArchiveFindings",
    "guardduty:GetFindings",
    "guardduty:ListDetectors"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecurityHubPermissions",
  "Effect" : "Allow",
```

```
    "Action" : [
      "securityHub:GetFindings"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDetectiveMemberAccess

AmazonDetectiveMemberAccess é uma [política gerenciada da AWS](#) que: fornece acesso de membro ao serviço Amazon Detective e acesso definido às dependências da interface do usuário do console.

### A utilização desta política

Você pode vincular a AmazonDetectiveMemberAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de janeiro de 2023, 15:16 UTC
- Horário editado: 17 de janeiro de 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess é uma [política gerenciada da AWS](#) que: fornece acesso às organizações para gerenciar o administrador delegado do Amazon Detective e acesso

com escopo às dependências da interface do usuário do console. Isso também concede permissão para criar uma função vinculada ao serviço para o Detective.

## A utilização desta política

Você pode vincular a `AmazonDetectiveOrganizationsAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de março de 2023, 15:20 UTC
- Horário editado: 02 de março de 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "detective.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "detective.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "detective.amazonaws.com",
```



```
        "guardduty.amazonaws.com",
        "macie.amazonaws.com",
        "securityhub.amazonaws.com"
    ]
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDetectiveServiceLinkedRolePolicy

AmazonDetectiveServiceLinkedRolePolicy é uma [política gerenciada da AWS](#) que: Permite que o Amazon Detective faça chamadas de serviço em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de novembro de 2021, 19:47 UTC
- Horário de edição: 18 de novembro de 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess é uma [política gerenciada da AWS](#) que: A política concede acesso total ao console do DevOps Guru.

## A utilização desta política

Você pode vincular a AmazonDevOpsGuruConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de dezembro de 2021, 18:43 UTC
- Horário de criação: 25 de agosto de 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
```

```
    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsListTopicsAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SnsTopicOperations",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:GetTopicAttributes",
      "sns:SetTopicAttributes",
      "sns:Publish"
    ],
    "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
  },
  {
    "Sid" : "DevOpsGuruSlrCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "devops-guru.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DevOpsGuruSlrDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PerformanceInsightsMetricsDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "pi:GetResourceMetrics",
      "pi:DescribeDimensionKeys"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsFilterLogEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon DevOps Guru.

### A utilização desta política

Você pode vincular a AmazonDevOpsGuruFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 16:38 UTC
- Horário de criação: 25 de agosto de 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
      "Condition" : {
```

```

    "StringLike" : {
      "iam:AWSServiceName" : "devops-guru.amazonaws.com"
    }
  },
  {
    "Sid" : "DevOpsGuruSlrDeletion",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsFilterLogEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs::*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)



- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess é uma [política gerenciada da AWS](#) que: fornece acesso para habilitar e gerenciar o Amazon DevOps Guru dentro de uma organização.

### A utilização desta política

Você pode vincular a AmazonDevOpsGuruOrganizationsAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de novembro de 2021, 23:50 UTC
- Horário de edição: 15 de novembro de 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "devops-guru:DescribeOrganizationHealth",
    "devops-guru:DescribeOrganizationResourceCollectionHealth",
    "devops-guru:DescribeOrganizationOverview",
    "devops-guru:ListOrganizationInsights",
    "devops-guru:SearchOrganizationInsights"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OrganizationsDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListRoots"
  ],
  "Resource" : "arn:aws:organizations::*:"
},
{
  "Sid" : "OrganizationsAdminDataAccess",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "devops-guru.amazonaws.com"
      ]
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura ao console do Amazon DevOps Guru.

### A utilização desta política

Você pode vincular a AmazonDevOpsGuruReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 16:34 UTC
- Horário de edição: 25 de agosto de 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Sid" : "DevOpsGuruReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "devops-guru:DescribeAccountHealth",
    "devops-guru:DescribeAccountOverview",
    "devops-guru:DescribeAnomaly",
    "devops-guru:DescribeEventSourcesConfig",
    "devops-guru:DescribeFeedback",
    "devops-guru:DescribeInsight",
    "devops-guru:DescribeResourceCollectionHealth",
    "devops-guru:DescribeServiceIntegration",
    "devops-guru:GetCostEstimation",
    "devops-guru:GetResourceCollection",
    "devops-guru:ListAnomaliesForInsight",
    "devops-guru:ListEvents",
    "devops-guru:ListInsights",
    "devops-guru:ListAnomalousLogGroups",
    "devops-guru:ListMonitoredResources",
    "devops-guru:ListNotificationChannels",
    "devops-guru:ListRecommendations",
    "devops-guru:SearchInsights",
    "devops-guru:StartCostEstimation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudFormationListStacksAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
},
{
```

```
    "Sid" : "CloudWatchGetMetricDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RDSDescribeDBInstancesAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsFilterLogEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy é uma [política gerenciada da AWS](#) que: é necessária uma função vinculada ao serviço para que o Amazon DevOps Gur acesse atributos em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 01 de dezembro de 2020, 10:24 UTC
- Horário de edição: 10 de janeiro de 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

## Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
```

```
"cloudwatch:DescribeAlarms",
"cloudwatch:ListDashboards",
"cloudwatch:GetDashboard",
"cloudformation:GetTemplate",
"cloudformation:ListStacks",
"cloudformation:ListStackResources",
"cloudformation:DescribeStacks",
"cloudformation:ListImports",
"codedeploy:BatchGetDeployments",
"codedeploy:GetDeploymentGroup",
"codedeploy:ListDeployments",
"config:DescribeConfigurationRecorderStatus",
"config:GetResourceConfigHistory",
"events:ListRuleNamesByTarget",
"xray:GetServiceGraph",
"organizations:ListRoots",
"organizations:ListChildren",
"organizations:ListDelegatedAdministrators",
"pi:GetResourceMetrics",
"tag:GetResources",
"lambda:GetFunction",
"lambda:GetFunctionConcurrency",
"lambda:GetAccountSettings",
"lambda:ListProvisionedConcurrencyConfigs",
"lambda:ListAliases",
"lambda:ListEventSourceMappings",
"lambda:GetPolicy",
"ec2:DescribeSubnets",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"sqs:GetQueueAttributes",
"kinesis:DescribeStream",
"kinesis:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeLimits",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeStream",
"dynamodb:ListStreams",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"rds:DescribeDBInstances",
"rds:DescribeDBClusters",
"rds:DescribeOptionGroups",
"rds:DescribeDBClusterParameters",
```

```

    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeAccountAttributes",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowPutTargetsOnASpecificRule",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
},
{
  "Sid" : "AllowCreateOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateOpsItem"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowAddTagsToOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:opsitem/*"
}

```



```
},
{
  "Sid" : "AllowAccessOpsItem",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetOpsItem",
    "ssm:UpdateOpsItem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
    }
  }
},
{
  "Sid" : "AllowCreateManagedRule",
  "Effect" : "Allow",
  "Action" : "events:PutRule",
  "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
},
{
  "Sid" : "AllowAccessManagedRule",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
},
{
  "Sid" : "AllowOtherOperationsOnManagedRule",
  "Effect" : "Allow",
  "Action" : [
    "events>DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "devops-guru.amazonaws.com"
    }
  }
}
```

```

    }
  },
  {
    "Sid" : "AllowTagBasedFilterLogEvents",
    "Effect" : "Allow",
    "Action" : [
      "logs:FilterLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
      }
    }
  },
  {
    "Sid" : "AllowAPIGatewayGetIntegrations",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis/????????????",
      "arn:aws:apigateway:*:*/restapis/*/resources",
      "arn:aws:apigateway:*:*/restapis/*/resources/*/methods/*/integration"
    ]
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole é uma [política gerenciada da AWS](#) que: fornece acesso ao upload de registros de replicação do DMS para os registros do cloudwatch na conta do cliente.

## A utilização desta política

Você pode vincular a `AmazonDMSCloudWatchLogsRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de janeiro de 2016, 23:44 UTC
- Horário de criação: 23 de maio de 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
      ],
    }
  ]
}
```

```

    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
    ]
  },
  {
    "Sid" : "AllowCreationOfDmsLogGroups",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
    ]
  },
  {
    "Sid" : "AllowCreationOfDmsLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ]
  },
  {
    "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
      "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
    ]
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDMSRedshiftS3Role

AmazonDMSRedshiftS3Role é uma [política gerenciada da AWS](#) que: fornece acesso para gerenciar as configurações do S3 dos endpoints do Redshift para DMS.

### A utilização desta política

Você pode vincular a AmazonDMSRedshiftS3Role aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de abril de 2016, 17:05 UTC
- Horário de edição: 08 de julho de 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3>DeleteBucket",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject",
      "s3:GetObjectVersion",
      "s3:GetBucketPolicy",
      "s3:PutBucketPolicy",
      "s3:GetBucketAcl",
      "s3:PutBucketVersioning",
      "s3:GetBucketVersioning",
      "s3:PutLifecycleConfiguration",
      "s3:GetLifecycleConfiguration",
      "s3>DeleteBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::dms-*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole é uma [política gerenciada da AWS](#) que: fornece acesso para gerenciar configurações de VPC para configurações gerenciadas de clientes de AWS

## A utilização desta política

Você pode vincular a `AmazonDMSVPCManagementRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 18 de novembro de 2015, 16:33 UTC
- Horário de criação: 23 de maio de 2016, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDB-ElasticServiceRolePolicy

AmazonDocDB-ElasticServiceRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon DocumentDB-Elastic gerencie atributos de AWS em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de novembro de 2022, 14:17 UTC
- Horário de edição: 30 de novembro de 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDBConsoleFullAccess

AmazonDocDBConsoleFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total para gerenciar o Amazon DocumentDB compatível com MongoDB usando o AWS Management Console. Importante notar que essa política também proporciona acesso total para publicação em todos os tópicos SNS da conta, permissões para criar e modificar instâncias do Amazon EC2 e configurações de VPC, autorizações para visualizar e listar chaves no Amazon KMS, além de acesso completo ao Amazon RDS e ao Amazon Neptune.

## A utilização desta política

Você pode vincular a AmazonDocDBConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de janeiro de 2019, 20:37 UTC
- Horário de edição: 30 de novembro de 2022, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "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:RemoveTagsForResource",
    "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"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDBElasticFullAccess

AmazonDocDBElasticFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total aos clusters elásticos do Amazon DocumentDB e outras permissões necessárias para suas dependências, incluindo EC2, KMS, SecretsManager, CloudWatch e IAM.

## A utilização desta política

Você pode vincular a `AmazonDocDBElasticFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de junho de 2023, 13:51 UTC
- Horário de edição: 21 de junho de 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDBElasticReadOnlyAccess

AmazonDocDBElasticReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura às métricas do Amazon DocDB-Elastic e do CloudWatch.

### A utilização desta política

Você pode vincular a AmazonDocDBElasticReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de junho de 2023, 14:37 UTC

- Horário de criação: 21 de junho de 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDBFullAccess

AmazonDocDBFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total para gerenciar o Amazon DocumentDB compatível com MongoDB. É importante observar que esta política também proporciona acesso total para a publicação em todos os tópicos do SNS dentro da conta, além de acesso completo ao Amazon RDS e ao Amazon Neptune.

### A utilização desta política

Você pode vincular a AmazonDocDBFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de janeiro de 2019, 20:21 UTC
- Horário de edição: 09 de janeiro de 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "rds:AddRoleToDBCluster",
      "rds:AddSourceIdentifierToSubscription",
      "rds:AddTagsToResource",
      "rds:ApplyPendingMaintenanceAction",
      "rds:CopyDBClusterParameterGroup",
      "rds:CopyDBClusterSnapshot",
      "rds:CopyDBParameterGroup",
      "rds:CreateDBCluster",
      "rds:CreateDBClusterParameterGroup",
      "rds:CreateDBClusterSnapshot",
      "rds:CreateDBInstance",
      "rds:CreateDBParameterGroup",
      "rds:CreateDBSubnetGroup",
      "rds:CreateEventSubscription",
      "rds>DeleteDBCluster",
      "rds>DeleteDBClusterParameterGroup",
      "rds>DeleteDBClusterSnapshot",
      "rds>DeleteDBInstance",
      "rds>DeleteDBParameterGroup",
      "rds>DeleteDBSubnetGroup",
      "rds>DeleteEventSubscription",
      "rds:DescribeAccountAttributes",
      "rds:DescribeCertificates",
      "rds:DescribeDBClusterParameterGroups",
      "rds:DescribeDBClusterParameters",
      "rds:DescribeDBClusterSnapshotAttributes",
      "rds:DescribeDBClusterSnapshots",
      "rds:DescribeDBClusters",
      "rds:DescribeDBEngineVersions",
      "rds:DescribeDBInstances",
      "rds:DescribeDBLogFiles",
      "rds:DescribeDBParameterGroups",
      "rds:DescribeDBParameters",
      "rds:DescribeDBSecurityGroups",
      "rds:DescribeDBSubnetGroups",
      "rds:DescribeEngineDefaultClusterParameters",
      "rds:DescribeEngineDefaultParameters",
      "rds:DescribeEventCategories",
      "rds:DescribeEventSubscriptions",
      "rds:DescribeEvents",
```

```

    "rds:DescribeOptionGroups",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DescribeValidDBInstanceModifications",
    "rds:DownloadDBLogFilePortion",
    "rds:FailoverDBCluster",
    "rds:ListTagsForResource",
    "rds:ModifyDBCluster",
    "rds:ModifyDBClusterParameterGroup",
    "rds:ModifyDBClusterSnapshotAttribute",
    "rds:ModifyDBInstance",
    "rds:ModifyDBParameterGroup",
    "rds:ModifyDBSubnetGroup",
    "rds:ModifyEventSubscription",
    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds: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"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDocDBReadOnlyAccess

AmazonDocDBReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso de somente leitura para gerenciar o Amazon DocumentDB compatível com MongoDB. Observe que essa política também concede acesso aos atributos do Amazon RDS e do Amazon Neptune.

## A utilização desta política

Você pode vincular a `AmazonDocDBReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de janeiro de 2019, 20:30 UTC
- Horário de edição: 09 de janeiro de 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
```



```

    "rds:DescribeEventSubscriptions",
    "rds:DescribeEvents",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DownloadDBLogFilePortion",
    "rds:ListTagsForResource"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "kms:ListAliases",
    "kms:ListKeyPolicies"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "logs:DescribeLogStreams",

```

```
    "logs:GetLogEvents"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
    "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDRSVPCManagement

AmazonDRSVPCManagement é uma [política gerenciada da AWS](#) que: fornece acesso para gerenciar configurações de VPC para configurações gerenciadas de clientes

### A utilização desta política

Você pode vincular a AmazonDRSVPCManagement aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de setembro de 2015, 00:09 UTC
- Horário de edição: 02 de setembro de 2015, 00:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDynamoDBFullAccess

AmazonDynamoDBFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon DynamoDB por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonDynamoDBFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 29 de janeiro de 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

### Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
```

```
"application-autoscaling:DescribeScalingActivities",
"application-autoscaling:DescribeScalingPolicies",
"application-autoscaling:PutScalingPolicy",
"application-autoscaling:RegisterScalableTarget",
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarmHistory",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:PutMetricAlarm",
"cloudwatch:GetMetricData",
"datapipeline:ActivatePipeline",
"datapipeline:CreatePipeline",
"datapipeline>DeletePipeline",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:PutPipelineDefinition",
"datapipeline:QueryObjects",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups",
"iam:GetRole",
"iam:ListRoles",
"kms:DescribeKey",
"kms:ListAliases",
"sns:CreateTopic",
"sns>DeleteTopic",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:Subscribe",
"sns:Unsubscribe",
"sns:SetTopicAttributes",
"lambda:CreateFunction",
"lambda:ListFunctions",
"lambda:ListEventSourceMappings",
"lambda:CreateEventSourceMapping",
"lambda>DeleteEventSourceMapping",
"lambda:GetFunctionConfiguration",
"lambda>DeleteFunction",
"resource-groups:ListGroups",
```

```

    "resource-groups:ListGroupResources",
    "resource-groups:GetGroup",
    "resource-groups:GetGroupQuery",
    "resource-groups>DeleteGroup",
    "resource-groups:CreateGroup",
    "tag:GetResources",
    "kinesis:ListStreams",
    "kinesis:DescribeStream",
    "kinesis:DescribeStreamSummary"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : "cloudwatch:GetInsightRuleReport",
  "Effect" : "Allow",
  "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "application-autoscaling.amazonaws.com",
        "application-autoscaling.amazonaws.com.cn",
        "dax.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "replication.dynamodb.amazonaws.com",

```

```
        "dax.amazonaws.com",
        "dynamodb.application-autoscaling.amazonaws.com",
        "contributorinsights.dynamodb.amazonaws.com",
        "kinesisreplication.dynamodb.amazonaws.com"
    ]
  }
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDynamoDBFullAccesswithDataPipeline

AmazonDynamoDBFullAccesswithDataPipeline é uma [política gerenciada da AWS](#) que: Essa política está em um caminho de suspensão de uso. Consulte a documentação para obter orientação: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>. Fornece acesso total ao Amazon DynamoDB, incluindo exportação/importação AWS usando o Data Pipeline por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonDynamoDBFullAccesswithDataPipeline aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 12 de novembro de 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```



```
    "Sid" : "DDBConsoleTriggers"
  },
  {
    "Action" : [
      "datapipeline:*",
      "iam:ListRoles"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Sid" : "DDBConsoleImportExport"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRolePolicy",
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Sid" : "IAMEDPRoles"
  },
  {
    "Action" : [
      "ec2:CreateTags",
      "ec2:DescribeInstances",
      "ec2:RunInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "elasticmapreduce:*",
      "datapipeline:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Sid" : "EMR"
  },
  {
    "Action" : [
      "s3:DeleteObject",
      "s3:Get*",
      "s3:List*",
      "s3:Put*"
    ],
  },
```

```
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ],
    "Sid" : "S3"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonDynamoDBReadOnlyAccess

AmazonDynamoDBReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon DynamoDB por meio do. AWS Management Console

### Utilização desta política

Você pode vincular a AmazonDynamoDBReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 20 de março de 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb: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*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy é uma [política gerenciada da AWS](#) que: política do IAM que permite que a conta do serviço de driver da CSI faça chamadas para serviços relacionados, como o EC2, em seu nome.

## A utilização desta política

Você pode vincular a AmazonEBSCSIDriverPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 04 de abril de 2022, 17:24 UTC
- Horário de edição: 18 de novembro de 2022, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonEC2ContainerRegistryFullAccess

AmazonEC2ContainerRegistryFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso administrativo aos atributos do Amazon ECR

## A utilização desta política

Você pode vincular a AmazonEC2ContainerRegistryFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de dezembro de 2015, 17:06 UTC
- Horário de edição: 05 de dezembro de 2020, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "replication.ecr.amazonaws.com"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerRegistryPowerUser

AmazonEC2ContainerRegistryPowerUser é uma [política gerenciada da AWS](#) que: Fornece acesso total aos repositórios do Amazon EC2 Container Registry, mas não permite a exclusão do repositório ou alterações nas políticas.

### A utilização desta política

Você pode vincular a AmazonEC2ContainerRegistryPowerUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 21 de dezembro de 2015, 17:05 UTC
- Horário de edição: 10 de dezembro de 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerRegistryReadOnly

AmazonEC2ContainerRegistryReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura aos repositórios do Amazon EC2 Container Registry.

### A utilização desta política

Você pode vincular a AmazonEC2ContainerRegistryReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de dezembro de 2015, 17:04 UTC
- Horário de edição 10 de dezembro de 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:GetRepositoryPolicy",
      "ecr:DescribeRepositories",
      "ecr:ListImages",
      "ecr:DescribeImages",
      "ecr:BatchGetImage",
      "ecr:GetLifecyclePolicy",
      "ecr:GetLifecyclePolicyPreview",
      "ecr:ListTagsForResource",
      "ecr:DescribeImageScanFindings"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole é uma [política gerenciada da AWS](#) que: Política para habilitar o escalonamento automático de tarefas para o Amazon EC2 Container Service

### A utilização desta política

Você pode vincular a AmazonEC2ContainerServiceAutoscaleRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 12 de maio de 2016, 23:25 UTC
- Horário de edição: 05 de fevereiro de 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
 ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerServiceEventsRole

AmazonEC2ContainerServiceEventsRole é uma [política gerenciada da AWS](#) que: Política para habilitar o CloudWatch Events para o EC2 Container Service

### A utilização desta política

Você pode vincular a AmazonEC2ContainerServiceEventsRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 30 de maio de 2017, 16:51 UTC
- Horário de edição: 06 de março de 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerServiceforEC2Role

AmazonEC2ContainerServiceforEC2Role é uma [política gerenciada da AWS](#) que: Política padrão para a função do Amazon EC2 para o Amazon EC2 Container Service.

### A utilização desta política

Você pode vincular a AmazonEC2ContainerServiceforEC2Role aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de março de 2015, 18:45 UTC
- Horário de edição: 06 de março de 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeTags",
      "ecs:CreateCluster",
      "ecs:DeregisterContainerInstance",
      "ecs:DiscoverPollEndpoint",
      "ecs:Poll",
      "ecs:RegisterContainerInstance",
      "ecs:StartTelemetrySession",
      "ecs:UpdateContainerInstancesState",
      "ecs:Submit*",
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ecs:TagResource",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ecs:CreateAction" : [
          "CreateCluster",
          "RegisterContainerInstance"
        ]
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ContainerServiceRole

AmazonEC2ContainerServiceRole é uma [política gerenciada da AWS](#) que: política padrão para a função de serviço Amazon ECS.

### A utilização desta política

Você pode vincular a AmazonEC2ContainerServiceRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de abril de 2015, 16:14 UTC
- Horário de edição: 11 de agosto de 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:Describe*",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:DeregisterTargets",
    "elasticloadbalancing:Describe*",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2FullAccess

AmazonEC2FullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon EC2 por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonEC2FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 27 de novembro de 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
```

```
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "transitgateway.amazonaws.com"
    ]
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon EC2 por meio do. AWS Management Console

### Utilização desta política

Você pode vincular a AmazonEC2ReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 14 de fevereiro de 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy é uma [política gerenciada da AWS](#) que: fornece acesso do EC2 ao bucket do S3 para baixar a revisão. Essa função é necessária para o atendente do CodeDeploy em instâncias do EC2.

### A utilização desta política

Você pode vincular a AmazonEC2RoleforAWSCodeDeploy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de maio de 2015, 18:10 UTC
- Horário de edição: 20 de março de 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
    },
  ],
}
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2RoleforAWSCodeDeployLimited

AmazonEC2RoleforAWSCodeDeployLimited é uma [política gerenciada da AWS](#) que: fornece acesso limitado do EC2 ao bucket do S3 para baixar a revisão. Essa função é necessária para o atendente do CodeDeploy em instâncias do EC2.

### A utilização desta política

Você pode vincular a AmazonEC2RoleforAWSCodeDeployLimited aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de agosto de 2020, 17:55 UTC
- Horário de edição: 20 de janeiro de 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole é uma [política gerenciada da AWS](#) que: política padrão para a perfil de serviço do Amazon EC2 para o Data Pipeline.

## A utilização desta política

Você pode vincular a AmazonEC2RoleforDataPipelineRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário de edição: 22 de fevereiro de 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
```

```
    "elasticmapreduce:ModifyInstanceGroups",
    "rds:Describe*",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSecurityGroups",
    "s3:*",
    "sdb:*",
    "sns:*",
    "sqs:*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2RoleforSSM

AmazonEC2RoleforSSM é uma [política gerenciada da AWS](#) que: Essa política estará obsoleta em breve. Use a política AmazonSSMManagedInstanceCore para ativar a funcionalidade do núcleo do serviço AWS Systems Manager em instâncias EC2. Para obter mais informações, consulte <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

## A utilização desta política

Você pode vincular a AmazonEC2RoleforSSM aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 29 de maio de 2015, 17:48 UTC

- Horário de edição: 24 de janeiro de 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
```

```
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2messages:AcknowledgeMessage",
    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",
    "ds:DescribeDirectories"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
```

```
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetEncryptionConfiguration",
      "s3:AbortMultipartUpload",
      "s3:ListMultipartUploadParts",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2RolePolicyForLaunchWizard

AmazonEC2RolePolicyForLaunchWizard é uma [política gerenciada da AWS](#) que: política gerenciada para a perfil de serviço Amazon LaunchWizard para EC2

### A utilização desta política

Você pode vincular a AmazonEC2RolePolicyForLaunchWizard aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de novembro de 2019, 08:05 UTC
- Horário de edição: 16 de maio de 2022, 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

## Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
```



```

    "Action" : [
      "ec2:ReplaceRoute"
    ],
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:AssociateAddress",
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeRegions",
      "ec2:DescribeVolumes",
      "ec2:DescribeRouteTables",
      "ec2:ModifyInstanceAttribute",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:PutMetricData",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2:CreateVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "LaunchWizardResourceGroupID",
          "LaunchWizardApplicationType"
        ]
      }
    }
  }
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:PutObjectTagging",
      "s3:GetBucketLocation",
      "logs:PutLogEvents",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:*",
      "arn:aws:s3:::launchwizard*",
      "arn:aws:s3:::aws-sap-data-provider/config.properties"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:Create*",
    "Resource" : "arn:aws:logs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:Describe*",
      "cloudformation:DescribeStackResources",
      "cloudformation:SignalResource",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "LaunchWizardResourceGroupID"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:BatchGetItem",
      "dynamodb:PutItem",
      "sqs:ReceiveMessage",

```

```

    "sqs:SendMessage",
    "dynamodb:Scan",
    "s3:ListBucket",
    "dynamodb:Query",
    "dynamodb:UpdateItem",
    "dynamodb>DeleteTable",
    "dynamodb>CreateTable",
    "s3:GetObject",
    "dynamodb:DescribeTable",
    "s3:GetBucketLocation",
    "dynamodb:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:dynamodb:*:*:table/LaunchWizard*",
    "arn:aws:sqs:*:*:LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/LaunchWizardApplicationType" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:GetDocument"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems",
    "fsx:ListTagsForResource",
    "fsx:DescribeStorageVirtualMachines"
  ]
}

```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : "LaunchWizard*"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2SpotFleetAutoscaleRole

AmazonEC2SpotFleetAutoscaleRole é uma [política gerenciada da AWS](#) que: Política para habilitar o escalonamento automático de tarefas para o Amazon EC2 Spot Fleet

### A utilização desta política

Você pode vincular a AmazonEC2SpotFleetAutoscaleRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de agosto de 2016, 18:27 UTC
- Horário de edição: 18 de fevereiro de 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEC2SpotFleetTaggingRole

AmazonEC2SpotFleetTaggingRole é uma [política gerenciada da AWS](#) que: permite que o EC2 Spot Fleet solicite, encerre e marque instâncias spot em seu nome.

### A utilização desta política

Você pode vincular a AmazonEC2SpotFleetTaggingRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 29 de junho de 2017, 18:19 UTC
- Horário de edição: 23 de abril de 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonECS\_FullAccess

AmazonECS\_FullAccess é uma [política gerenciada da AWS](#) que: fornece acesso administrativo aos recursos do Amazon ECS e ativa os recursos do ECS através do acesso a outros recursos de serviço da AWS, como VPCs, grupos de ajuste de escala automático e pilhas do CloudFormation.

### A utilização desta política

Você pode vincular a AmazonECS\_FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de novembro de 2017, 21:36 UTC
- Horário de edição: 04 de janeiro de 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`



## Versão da política

Versão da política: v20 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "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"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity é uma [política AWS gerenciada](#) que: fornece acesso administrativo à Autoridade de Certificação Privada, ao AWS Secrets Manager e a outros recursos Serviços da AWS necessários para gerenciar os recursos TLS do ECS Service Connect em seu nome.

## Utilização desta política

Você pode vincular a

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 19 de janeiro de 2024, 20:08 UTC
- Horário editado: 19 de janeiro de 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        }
      },
      "StringEquals" : {
```

```

        "aws:RequestTag/AmazonECSTagged" : "true",
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
},
{
    "Sid" : "TagOnCreateSecret",
    "Effect" : "Allow",
    "Action" : "secretsmanager:TagResource",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
    "Condition" : {
        "ArnLike" : {
            "aws:RequestTag/AmazonECSTagged" : [
                "arn:aws:ecs:*:*:service/*/*",
                "arn:aws:ecs:*:*:task-set/*/*"
            ]
        },
        "StringEquals" : {
            "aws:RequestTag/AmazonECSTagged" : "true",
            "aws:ResourceAccount" : "${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"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonECSInfrastructureRolePolicyForVolumes

AmazonECSInfrastructureRolePolicyForVolumes é uma [política AWS gerenciada](#) que: fornece acesso a outros recursos AWS de serviço necessários para gerenciar volumes associados às cargas de trabalho do ECS em seu nome.

## Utilização desta política

Você pode vincular a AmazonECSInfrastructureRolePolicyForVolumes aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 10 de janeiro de 2024, 22:56 UTC
- Horário editado: 10 de janeiro de 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
```

```

    "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
  },
  "StringEquals" : {
    "aws:RequestTag/AmazonECSManaged" : "true"
  }
},
{
  "Sid" : "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/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Política para permitir que o Amazon ECS gerencie seu cluster.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de outubro de 2017, 01:18 UTC
- Horário editado: 04 de dezembro de 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*"
      ]
    }
  ]
}
```

```

    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:RegisterTargets",
    "route53:ChangeResourceRecordSets",
    "route53:CreateHealthCheck",
    "route53>DeleteHealthCheck",
    "route53:Get*",
    "route53:List*",
    "route53:UpdateHealthCheck",
    "servicediscovery:DeregisterInstance",
    "servicediscovery:Get*",
    "servicediscovery:List*",
    "servicediscovery:RegisterInstance",
    "servicediscovery:UpdateInstanceCustomHealthStatus"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScaling",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AutoScalingManagement",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:SetInstanceProtection",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:PutLifecycleHook",
    "autoscaling>DeleteLifecycleHook",
    "autoscaling:CompleteLifecycleAction",
    "autoscaling:RecordLifecycleActionHeartbeat"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "autoscaling:ResourceTag/AmazonECSManaged" : "false"
    }
  }
}
},

```

```
{
  "Sid" : "AutoScalingPlanManagement",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling-plans:CreateScalingPlan",
    "autoscaling-plans>DeleteScalingPlan",
    "autoscaling-plans:DescribeScalingPlans",
    "autoscaling-plans:DescribeScalingPlanResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EventBridge",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
},
{
  "Sid" : "EventBridgeRuleManagement",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "ecs.amazonaws.com"
    }
  }
},
{
  "Sid" : "CWAlarmManagement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch>DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
},
```

```
{
  "Sid" : "ECSTagging",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "CWLogGroupManagement",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
},
{
  "Sid" : "CWLogStreamManagement",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
},
{
  "Sid" : "ExecuteCommandSessionManagement",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeSessions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ExecuteCommand",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : [
    "arn:aws:ecs:*:*:task/*",
```



```
    "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
  ],
},
{
  "Sid" : "CloudMapResourceCreation",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:CreateHttpNamespace",
    "servicediscovery:CreateService"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AmazonECSManaged"
      ]
    }
  }
},
{
  "Sid" : "CloudMapResourceTagging",
  "Effect" : "Allow",
  "Action" : "servicediscovery:TagResource",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AmazonECSManaged" : "*"
    }
  }
},
{
  "Sid" : "CloudMapResourceDeletion",
  "Effect" : "Allow",
  "Action" : [
    "servicediscovery:DeleteService"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonECSManaged" : "false"
    }
  }
},
{
```

```
    "Sid" : "CloudMapResourceDiscovery",
    "Effect" : "Allow",
    "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy é uma [política gerenciada da AWS](#) que: Fornece acesso a outros atributos de serviço de AWS necessários para executar tarefas do Amazon ECS

### A utilização desta política

Você pode vincular a AmazonECSTaskExecutionRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 16 de novembro de 2017, 18:48 UTC
- Horário de edição: 16 de novembro de 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy é uma [política gerenciada da AWS](#) que: fornece acesso de gerenciamento aos recursos do EFS e acesso de leitura ao EC2

## A utilização desta política

Você pode vincular a `AmazonEFSCSIDriverPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 25 de julho de 2023, 20:10 UTC
- Horário de edição: 25 de julho de 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowTagNewAccessPoints",
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticfilesystem:CreateAction" : "CreateAccessPoint"
      },
      "Null" : {
        "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "efs.csi.aws.com/cluster"
      }
    }
  },
  {
    "Sid" : "AllowDeleteAccessPoint",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:DeleteAccessPoint",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKS\_CNI\_Policy

AmazonEKS\_CNI\_Policy é uma [política AWS gerenciada](#) que: Essa política fornece ao Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) as permissões necessárias para modificar a configuração do endereço IP nos nós de trabalho do EKS. Esse conjunto de permissões permite que o CNI liste, descreva e modifique o Elastic Network Interfaces em seu nome. Mais informações sobre o plug-in AWS VPC CNI estão disponíveis aqui: <https://github.com/aws/8s-amazon-vpc-cni-k>

## Utilização desta política

Você pode vincular a AmazonEKS\_CNI\_Policy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 27 de maio de 2018, 21:07 UTC
- Horário editado: 04 de março de 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonEKSClusterPolicy

AmazonEKSClusterPolicy é uma [política gerenciada da AWS](#) que: Essa política fornece ao Kubernetes as permissões necessárias para gerenciar recursos em seu nome. O Kubernetes requer permissões `Ec2:CreateTags` para colocar informações de identificação nos recursos do EC2, incluindo, entre outros, instâncias, grupos de segurança e interfaces de rede elásticas.

### A utilização desta política

Você pode vincular a AmazonEKSClusterPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2018, 21:06 UTC
- Horário de edição: 07 de fevereiro de 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEKSCoordinatorServiceRolePolicy

AmazonEKSCoordinatorServiceRolePolicy é uma [política gerenciada da AWS](#) que: Essa política permite que o Amazon EKS gerencie os atributos da AWS para o conector do EKS

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de setembro de 2021, 20:31 UTC
- Horário de edição: 04 de setembro de 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMServices",
      "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"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy é uma [política gerenciada da AWS](#) que: fornece acesso a outros AWS recursos de serviço que são necessários para executar pods do Amazon EKS no AWS Fargate

### A utilização desta política

Você pode vincular a AmazonEKSFargatePodExecutionRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 22 de novembro de 2019, 04:34 UTC
- Horário de edição: 22 de novembro de 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEKSFargateServiceRolePolicy

AmazonEKSFargateServiceRolePolicy é uma [AWS política gerenciada](#) que concede permissões necessárias ao Amazon EKS para executar tarefas do Fargate

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 22 de novembro de 2019, 04:36 UTC
- Horário de edição: 22 de novembro de 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy é uma [política gerenciada da AWS](#) que: Essa política fornece permissões para que as instâncias do ambiente de gerenciamento do cluster local do EKS executadas em sua conta gerenciem recursos em seu nome.

### A utilização desta política

Você pode vincular a AmazonEKSLocalOutpostClusterPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de agosto de 2022, 21:56 UTC
- Horário de edição: 17 de outubro de 2022, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

### Versão da política

Versão da política: v3 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSLocalOutpostServiceRolePolicy

AmazonEKSLocalOutpostServiceRolePolicy é uma [política gerenciada da AWS](#) que: Permite que o Amazon EKS Local faça a chamada dos serviços de AWS em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de agosto de 2022, 21:53 UTC
- Horário de edição: 24 de outubro de 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeRouteTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribePlacementGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:security-group*"
  ]
}

```

```

    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:launch-template/*",

```

```

    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:placement-group*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:TerminateInstances",
    "ec2:GetConsoleOutput"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance*"
  ],
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*",
        "eks*"
      ]
    }
  },
  "StringEquals" : {
    "ec2:CreateAction" : [
      "CreateNetworkInterface",
      "CreateSecurityGroup",
      "RunInstances"
    ]
  }
}

```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*",
        "eks*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "secretsmanager:DeleteSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/eks-local:controlplane-name" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "secretsmanager:DescribeSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
}

```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ssm:resourceTag/eks-local:controlplane-name" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/AmazonEKS-ControlPlaneInstanceProxy"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```



```
        "ssm:ResumeSession",
        "ssm:TerminateSession"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:GetOutpost"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSServicePolicy

AmazonEKSServicePolicy é uma [política gerenciada da AWS](#): Essa política permite que o Amazon Elastic Container Service para Kubernetes crie e gereencie os atributos necessários para operar clusters do EKS.

### A utilização desta política

Você pode vincular a AmazonEKSServicePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2018, 21:08 UTC
- Horário de edição: 27 de maio de 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion"
      ],
      "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"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEKSServiceRolePolicy

AmazonEKSServiceRolePolicy é uma [política gerenciada da AWS](#) que: É necessária uma função vinculada ao serviço para que o Amazon EKS chame serviços de AWS em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de fevereiro de 2020, 20:10 UTC
- Horário de edição: 27 de maio de 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSVPCResourceController

AmazonEKSVPCResourceController é uma [política gerenciada da AWS](#) que: Política usada pelo VPC Resource Controller para gerenciar ENI e IPs para nós de trabalho.

### A utilização desta política

Você pode vincular a AmazonEKSVPCResourceController aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de agosto de 2020, 00:55 UTC
- Horário de edição: 12 de agosto de 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
        "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy é uma [política gerenciada pela AWS](#): Essa política permite que os nós de trabalho do Amazon EKS se conectem aos clusters do Amazon EKS.

### Utilização desta política

Você pode vincular a AmazonEKSWorkerNodePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS



- Horário de criação: 27 de maio de 2018, 21:09 UTC
- Horário editado: 27 de novembro de 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSEKWorkerNodePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElastiCacheFullAccess

AmazonElastiCacheFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à Amazon ElastiCache por meio do AWS Management Console.

### Utilização desta política

Você pode vincular a AmazonElastiCacheFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 28 de novembro de 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```

"Statement" : [
  {
    "Sid" : "ElastiCacheManagementActions",
    "Effect" : "Allow",
    "Action" : "elasticache:*",
    "Resource" : "*"
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "elasticache.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CreateVPCEndpoints",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : "arn:aws:ec2::*:vpc-endpoint/*",
    "Condition" : {
      "StringLike" : {
        "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
      }
    }
  },
  {
    "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2::*:vpc-endpoint/*"
  },
  {
    "Sid" : "TagVPCEndpointsOnCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
  },

```

```

    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AmazonElasticCacheManaged" : "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" : "*"
}
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElastiCacheReadOnlyAccess

AmazonElastiCacheReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon ElastiCache por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonElastiCacheReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticContainerRegistryPublicFullAccess

AmazonElasticContainerRegistryPublicFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso administrativo aos atributos do Amazon ECR Public

### A utilização desta política

Você pode vincular a AmazonElasticContainerRegistryPublicFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 17:25 UTC

- Horário de edição: 01 de dezembro de 2020, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser é uma [política gerenciada da AWS](#): fornece acesso total aos repositórios públicos do Amazon ECR, mas não permite a exclusão de repositórios ou alterações de políticas.

## A utilização desta política

Você pode vincular a AmazonElasticContainerRegistryPublicPowerUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 16:16 UTC
- Horário de edição: 01 de dezembro de 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
```

```
    "ecr-public:GetRepositoryPolicy",
    "ecr-public:DescribeRepositories",
    "ecr-public:DescribeRegistries",
    "ecr-public:DescribeImages",
    "ecr-public:DescribeImageTags",
    "ecr-public:GetRepositoryCatalogData",
    "ecr-public:GetRegistryCatalogData",
    "ecr-public:InitiateLayerUpload",
    "ecr-public:UploadLayerPart",
    "ecr-public:CompleteLayerUpload",
    "ecr-public:PutImage"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticContainerRegistryPublicReadOnly

AmazonElasticContainerRegistryPublicReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura aos repositórios do Amazon ECR Public.

### A utilização desta política

Você pode vincular a AmazonElasticContainerRegistryPublicReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 17:27 UTC

- Horário de edição: 01 de dezembro de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso ao cliente raiz a um sistema de arquivos Amazon EFS

### A utilização desta política

Você pode vincular a AmazonElasticFileSystemClientFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de janeiro de 2020, 16:27 UTC
- Horário de edição: 13 de janeiro de 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemClientReadOnlyAccess

AmazonElasticFileSystemClientReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso ao cliente somente leitura a um sistema de arquivos Amazon EFS

### A utilização desta política

Você pode vincular a AmazonElasticFileSystemClientReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de janeiro de 2020, 16:24 UTC
- Horário de edição: 13 de janeiro de 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemClientReadWriteAccess

AmazonElasticFileSystemClientReadWriteAccess é uma [política gerenciada da AWS](#) que: fornece acesso ao cliente de leitura e edição a um sistema de arquivos Amazon EFS

## A utilização desta política

Você pode vincular a AmazonElasticFileSystemClientReadWriteAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de janeiro de 2020, 16:21 UTC
- Horário de edição: 13 de janeiro de 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemFullAccess

AmazonElasticFileSystemFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total ao Amazon EFS por meio de AWS Management Console.

### Utilização desta política

Você pode vincular a AmazonElasticFileSystemFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 27 de maio de 2015, 16:22 UTC
- Horário editado: 28 de novembro de 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemReadOnlyAccess

AmazonElasticFileSystemReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EFS por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonElasticFileSystemReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2015, 16:25 UTC
- Horário de edição: 10 de janeiro de 2022, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemServiceRolePolicy

AmazonElasticFileSystemServiceRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon Elastic File System gerencie AWS recursos em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de novembro de 2019, 16:52 UTC
- Horário de edição: 10 de janeiro de 2022, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "backup:CreateBackupPlan",
      "backup:CreateBackupSelection"
    ],
    "Resource" : [
      "arn:aws:backup:*:*:backup-plan:*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "backup.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticfilesystem:DescribeFileSystems",
```

```
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem>DeleteReplicationConfiguration"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticFileSystemsUtils

AmazonElasticFileSystemsUtils é uma [política gerenciada da AWS](#) que: permite que os clientes usem o AWS Systems Manager para gerenciar automaticamente o pacote de utilitários Amazon EFS (amazon-efs-utils) em suas instâncias EC2 e usem o CloudWatchLog para obter notificações de sucesso/falha de montagem do sistema de arquivos EFS.

## A utilização desta política

Você pode vincular a AmazonElasticFileSystemsUtils aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de setembro de 2020, 15:16 UTC
- Horário de edição: 29 de setembro de 2020, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```



```
        "ec2messages:AcknowledgeMessage",
        "ec2messages>DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "elasticfilesystem:DescribeMountTargets"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeAvailabilityZones"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceEditorsRole

AmazonElasticMapReduceEditorsRole é uma [política gerenciada da AWS](#): política padrão para o perfil de serviço Amazon Elastic MapReduce Editors.

### A utilização desta política

Você pode vincular a AmazonElasticMapReduceEditorsRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Hora da criação: 16 de novembro de 2018, 21:55 UTC
- Horário de edição: 09 de fevereiro de 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:CreateNetworkInterface",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DescribeNetworkInterfaces",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeTags",
      "ec2:DescribeInstances",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "elasticmapreduce:ListInstances",
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:ListSteps"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "aws:elasticmapreduce:editor-id",
          "aws:elasticmapreduce:job-flow-id"
        ]
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceforAutoScalingRole

AmazonElasticMapReduceforAutoScalingRole é uma [política gerenciada da AWS](#) que: Amazon Elastic MapReduce para ajuste de escala automático. Função para permitir que o ajuste de escala automático adicione e remova instâncias do seu cluster EMR.

### A utilização desta política

Você pode vincular a AmazonElasticMapReduceforAutoScalingRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 18 de novembro de 2016, 01:09 UTC
- Horário de edição: 18 de novembro de 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ModifyInstanceGroups"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceforEC2Role

AmazonElasticMapReduceforEC2Role é uma [política gerenciada da AWS](#): política padrão para o perfil de serviço Amazon Elastic MapReduce para EC2.

### A utilização desta política

Você pode vincular a AmazonElasticMapReduceforEC2Role aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário de edição: 11 de agosto de 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue>DeleteDatabase",
        "glue:GetDatabase",

```

```
"glue:GetDatabases",
"glue:CreateTable",
"glue:UpdateTable",
"glue>DeleteTable",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersions",
"glue:CreatePartition",
"glue:BatchCreatePartition",
"glue:UpdatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:GetPartition",
"glue:GetPartitions",
"glue:BatchGetPartition",
"glue:CreateUserDefinedFunction",
"glue:UpdateUserDefinedFunction",
"glue>DeleteUserDefinedFunction",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceFullAccess

AmazonElasticMapReduceFullAccess é uma [política gerenciada da AWS](#) que: Essa política está em um caminho de suspensão de uso. Consulte a documentação para obter orientação: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Fornece acesso total ao Amazon Elastic MapReduce e aos serviços subjacentes necessários, como EC2 e S3

## A utilização desta política

Você pode vincular a `AmazonElasticMapReduceFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 11 de outubro de 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2>DeleteRoute",
        "ec2>DeleteTags",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
```



```

    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeRouteTables",
    "ec2:DescribeNetworkAcls",
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "elasticmapreduce:*",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:List*",
    "s3:*",
    "sdb:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [
        "elasticmapreduce.amazonaws.com",
        "elasticmapreduce.amazonaws.com.cn"
      ]
    }
  }
}
]

```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReducePlacementGroupPolicy

AmazonElasticMapReducePlacementGroupPolicy é uma [política gerenciada da AWS](#): Política para permitir que o EMR crie, descreva e exclua grupos de posicionamento do EC2.

### A utilização desta política

Você pode vincular a AmazonElasticMapReducePlacementGroupPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de setembro de 2020, 00:37 UTC
- Horário de edição: 29 de setembro de 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceReadOnlyAccess

AmazonElasticMapReduceReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Elastic MapReduce por meio de AWS Management Console.

## A utilização desta política

Você pode vincular a `AmazonElasticMapReduceReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 29 de julho de 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticMapReduceRole

AmazonElasticMapReduceRole é uma [política gerenciada da AWS](#) que: Essa política está em um caminho de suspensão de uso. Consulte a documentação para obter orientação: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>. Política padrão para o perfil de serviço do Amazon Elastic MapReduce.

## A utilização desta política

Você pode vincular a AmazonElasticMapReduceRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário de edição: 24 de junho de 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

## Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
```

```

    "ec2:ModifyImageAttribute",
    "ec2:ModifyInstanceAttribute",
    "ec2:RequestSpotInstances",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "ec2>DeleteVolume",
    "ec2:DescribeVolumeStatus",
    "ec2:DescribeVolumes",
    "ec2:DetachVolume",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListInstanceProfiles",
    "iam:ListRolePolicies",
    "iam:PassRole",
    "s3:CreateBucket",
    "s3:Get*",
    "s3:List*",
    "sdb:BatchPutAttributes",
    "sdb:Select",
    "sqs:CreateQueue",
    "sqs>Delete*",
    "sqs:GetQueue*",
    "sqs:PurgeQueue",
    "sqs:ReceiveMessage",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling>DeleteScalingPolicy",
    "application-autoscaling:Describe*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "spot.amazonaws.com"
    }
  }
}

```

```
    }  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticsearchServiceRolePolicy

AmazonElasticsearchServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite que o Amazon Elasticsearch Service acesse outros serviços de AWS, como APIs de rede do EC2 em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de julho de 2017, 00:15 UTC
- Horário de edição: 23 de outubro de 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    }
  ]
}
```

```
},
{
  "Sid" : "Stmt1480452973198",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "Stmt1480452973199",
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/OpenSearchManaged" : "true"
    }
  }
},
{
  "Sid" : "Stmt1480452973200",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/OpenSearchManaged" : "true"
    }
  }
},
{
  "Sid" : "Stmt1480452973201",
  "Effect" : "Allow",
  "Action" : [
```

```
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Stmt1480452973149",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973150",
  "Effect" : "Allow",
  "Action" : [
    "ec2:UnAssignIpv6Addresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Sid" : "Stmt1480452973202",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    }
  }
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonElasticTranscoder\_FullAccess

AmazonElasticTranscoder\_FullAccess é uma [política gerenciada da AWS](#) que: concede aos usuários acesso total ao Elastic Transcoder e o acesso aos serviços associados que são necessários para a funcionalidade completa do Elastic Transcoder.

## A utilização desta política

Você pode vincular a AmazonElasticTranscoder\_FullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de abril de 2018, 18:59 UTC
- Horário de edição: 10 de junho de 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
    },
  ],
}
```

```
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "elastictranscoder.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticTranscoder\_JobsSubmitter

AmazonElasticTranscoder\_JobsSubmitter é uma [política gerenciada da AWS](#) que: concede aos usuários permissão para alterar predefinições, enviar tarefas e visualizar as configurações do Elastic Transcoder. Essa política também concede acesso somente de leitura a alguns outros serviços necessários para usar o console do Elastic Transcode, incluindo S3, IAM e SNS.

## A utilização desta política

Você pode vincular a AmazonElasticTranscoder\_JobsSubmitter aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de junho de 2018, 21:12 UTC
- Horário de edição: 10 de junho de 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticTranscoder\_ReadOnlyAccess

AmazonElasticTranscoder\_ReadOnlyAccess é uma [política gerenciada da AWS](#) que: concede aos usuários acesso somente de leitura ao Elastic Transcoder e acesso à lista de serviços relacionados.

### A utilização desta política

Você pode vincular a AmazonElasticTranscoder\_ReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de junho de 2018, 21:09 UTC
- Horário de edição: 10 de junho de 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "elastictranscoder:Read*",
      "elastictranscoder:List*",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "iam:ListRoles",
      "sns:ListTopics"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonElasticTranscoderRole

AmazonElasticTranscoderRole é uma [política gerenciada da AWS](#): política padrão para o perfil de serviço Amazon Elastic Transcoder.

### A utilização desta política

Você pode vincular a AmazonElasticTranscoderRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário de edição: 13 de junho de 2019, 22:48 UTC



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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEMRCleanupPolicy

AmazonEMRCleanupPolicy é uma [política gerenciada da AWS](#) que: permite as ações que o EMR exige para encerrar e excluir atributos do AWS EC2 se o perfil de serviço do EMR tiver perdido essa capacidade.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de setembro de 2017, 23:54 UTC
- Horário de edição: 29 de setembro de 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Resource" : "*",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeSpotInstanceRequests",
      "ec2>DeleteLaunchTemplate",
      "ec2:ModifyInstanceAttribute",
      "ec2:TerminateInstances",
      "ec2:CancelSpotInstanceRequests",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVolumes",
      "ec2:DetachVolume",
      "ec2>DeleteVolume",
      "ec2:DescribePlacementGroups",
      "ec2>DeletePlacementGroup"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEMRContainersServiceRolePolicy

AmazonEMRContainersServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite acesso a outros atributos de serviço de AWS necessários para executar tarefas do Amazon EMR

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de dezembro de 2020, 00:38 UTC
- Horário de edição: 10 de março de 2023, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "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"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEMRFullAccessPolicy\_v2

AmazonEMRFullAccessPolicy\_v2 é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon EMR

## A utilização desta política

Você pode vincular a AmazonEMRFullAccessPolicy\_v2 aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 12 de março de 2021, 01:50 UTC
- Horário de edição: 28 de julho de 2023, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
```

```
"elasticmapreduce:AddTags",
"elasticmapreduce:CancelSteps",
"elasticmapreduce:CreateEditor",
"elasticmapreduce: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" : "*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEMRReadOnlyAccessPolicy\_v2

AmazonEMRReadOnlyAccessPolicy\_v2 é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EMR e às métricas associados do Cloudwatch.

## A utilização desta política

Você pode vincular a AmazonEMRReadOnlyAccessPolicy\_v2 aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 12 de março de 2021, 01:39 UTC
- Horário de edição: 02 de agosto de 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
```

```

    "elasticmapreduce:GetBlockPublicAccessConfiguration",
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:GetAutoTerminationPolicy",
    "elasticmapreduce:ListBootstrapActions",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListEditors",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "elasticmapreduce:ListSupportedInstanceTypes",
    "elasticmapreduce:ViewEventsFromAllClustersInConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ViewMetricsInEMRConsole",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEMRServerlessServiceRolePolicy

AmazonEMRServerlessServiceRolePolicy é uma [política gerenciada pela AWS](#) que: permite acesso a outros atributos de serviço de AWS necessários para executar tarefas do Amazon EMR sem servidor

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de maio de 2022, 23:15 UTC
- Horário editado: 25 de janeiro de 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchPolicyStatement",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/EMRServerless",
          "AWS/Usage"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEMRServicePolicy\_v2

AmazonEMRServicePolicy\_v2 é uma [política gerenciada da AWS](#): essa política é usada para o perfil de serviço do Amazon EMR e NÃO deve ser usada para nenhum outro usuário ou função do IAM em sua conta. A política concede permissões para criar e gerenciar recursos associados ao EMR e serviços relacionados necessários para a operação do seu cluster do EMR.

## A utilização desta política

Você pode vincular a AmazonEMRServicePolicy\_v2 aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Hora de criação: 12 de março de 2021, 01:11 UTC
- Horário de edição: 15 de fevereiro de 2022, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    }
  ],
}
```

```
{
  "Sid" : "CreateWithEMRTaggedLaunchTemplate",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateFleet",
    "ec2:RunInstances",
    "ec2:CreateLaunchTemplateVersion"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateEMRTaggedLaunchTemplate",
  "Effect" : "Allow",
  "Action" : "ec2:CreateLaunchTemplate",
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateEMRTaggedInstancesAndVolumes",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:CreateFleet"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
```

```

    "Sid" : "ResourcesToLaunchEC2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
    ]
},
{
    "Sid" : "ManageEMRTaggedResources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "ManageTagsOnEMRTaggedResources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Resource" : [

```



```

    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "TagOnCreateTaggedEMRResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateFleet",
        "CreateLaunchTemplate",

```

```
        "CreateNetworkInterface"
      ]
    }
  },
  {
    "Sid" : "TagPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:placement-group/EMR_*"
    ]
  },
  {
    "Sid" : "ListActionsForEC2Resources",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2: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*"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonESCognitoAccess

AmazonESCognitoAccess é uma [política gerenciada da AWS](#) que: fornece acesso limitado ao serviço de configuração do Amazon Cognito.

### A utilização desta política

Você pode vincular a AmazonESCognitoAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de fevereiro de 2018, 22:29 UTC
- Horário editado: 20 de dezembro de 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Action" : [
  "cognito-idp:DescribeUserPool",
  "cognito-idp:CreateUserPoolClient",
  "cognito-idp>DeleteUserPoolClient",
  "cognito-idp:UpdateUserPoolClient",
  "cognito-idp:DescribeUserPoolClient",
  "cognito-idp:AdminInitiateAuth",
  "cognito-idp:AdminUserGlobalSignOut",
  "cognito-idp:ListUserPoolClients",
  "cognito-identity:DescribeIdentityPool",
  "cognito-identity:UpdateIdentityPool",
  "cognito-identity:SetIdentityPoolRoles",
  "cognito-identity:GetIdentityPoolRoles"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "cognito-identity.amazonaws.com",
        "cognito-identity-us-gov.amazonaws.com"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonESFullAccess

AmazonESFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao serviço de configuração do Amazon ES.

## A utilização desta política

Você pode vincular a AmazonESFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de outubro de 2015, 19:14 UTC
- Horário de edição: 01 de outubro de 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonESReadOnlyAccess

AmazonESReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao serviço de configuração do Amazon ES.

### A utilização desta política

Você pode vincular a AmazonESReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de outubro de 2015, 19:18 UTC
- Horário de edição: 03 de outubro de 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "es:Describe*",
      "es:List*",
      "es:Get*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite que o EventBridge acesse os recursos do Secret Manager em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 11 de fevereiro de 2021, 20:52 UTC
- Horário de edição: 11 de fevereiro de 2021, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeFullAccess

AmazonEventBridgeFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon EventBridge.

## A utilização desta política

Você pode vincular a `AmazonEventBridgeFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de julho de 2019, 14:08 UTC
- Horário de edição: 01 de dezembro de 2022, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgePipesFullAccess

AmazonEventBridgePipesFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon EventBridge Pipes.

### A utilização desta política

Você pode vincular a AmazonEventBridgePipesFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2022, 17:03 UTC
- Horário de edição: 01 de dezembro de 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura e de operador (capacidade de parar e começar a executar Pipes) ao Amazon EventBridge Pipes.

### A utilização desta política

Você pode vincular a AmazonEventBridgePipesOperatorAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2022, 17:04 UTC
- Horário de edição: 01 de dezembro de 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "pipes:DescribePipe",
      "pipes:ListPipes",
      "pipes:ListTagsForResource",
      "pipes:StartPipe",
      "pipes:StopPipe"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgePipesReadOnlyAccess

AmazonEventBridgePipesReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EventBridge Pipes.

### A utilização desta política

Você pode vincular a AmazonEventBridgePipesReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2022, 17:04 UTC

- Horário de edição: 01 de dezembro de 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEventBridgeReadOnlyAccess

AmazonEventBridgeReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EventBridge.

## A utilização desta política

Você pode vincular a AmazonEventBridgeReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de julho de 2019, 13:59 UTC
- Horário de edição: 01 de dezembro de 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
```

```

    "events:TestEventPattern",
    "events:DescribeArchive",
    "events:ListArchives",
    "events:DescribeReplay",
    "events:ListReplays",
    "events:DescribeConnection",
    "events:ListConnections",
    "events:DescribeApiDestination",
    "events:ListApiDestinations",
    "events:DescribeEndpoint",
    "events:ListEndpoints",
    "schemas:DescribeCodeBinding",
    "schemas:DescribeDiscoverer",
    "schemas:DescribeRegistry",
    "schemas:DescribeSchema",
    "schemas:ExportSchema",
    "schemas:GetCodeBindingSource",
    "schemas:GetDiscoveredSchema",
    "schemas:GetResourcePolicy",
    "schemas:ListDiscoverers",
    "schemas:ListRegistries",
    "schemas:ListSchemas",
    "schemas:ListSchemaVersions",
    "schemas:ListTagsForResource",
    "schemas:SearchSchemas",
    "scheduler:GetSchedule",
    "scheduler:GetScheduleGroup",
    "scheduler:ListSchedules",
    "scheduler:ListScheduleGroups",
    "scheduler:ListTagsForResource",
    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeSchedulerFullAccess

AmazonEventBridgeSchedulerFullAccess é uma [política gerenciada da AWS](#) que: A política gerenciada de AmazonEventBridgeSchedulerFullAccess concede permissões para usar todas as ações do EventBridge Scheduler para agendas e grupos de agendas.

### A utilização desta política

Você pode vincular a AmazonEventBridgeSchedulerFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de novembro de 2022, 18:37 UTC
- Horário de edição: 10 de novembro de 2022, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : "scheduler:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "scheduler.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeSchedulerReadOnlyAccess

AmazonEventBridgeSchedulerReadOnlyAccess é uma [política gerenciada da AWS](#): a política gerenciada AmazonEventBridgeSchedulerReadOnlyAccess concede permissões somente leitura para exibir detalhes sobre suas agendas e grupos de agendas

### A utilização desta política

Você pode vincular a AmazonEventBridgeSchedulerReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 10 de novembro de 2022, 18:50 UTC
- Horário de edição: 10 de novembro de 2022, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonEventBridgeSchemasFullAccess

AmazonEventBridgeSchemasFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon EventBridge Schemas.

## A utilização desta política

Você pode vincular a AmazonEventBridgeSchemasFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de novembro de 2019, 23:12 UTC
- Horário de edição: 28 de novembro de 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



```

    "Sid" : "AmazonEventBridgeManageRule",
    "Effect" : "Allow",
    "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events>ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
  },
  {
    "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EventBridge Schemas.

### A utilização desta política

Você pode vincular a AmazonEventBridgeSchemasReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de novembro de 2019, 23:05 UTC
- Horário de edição: 01 de maio de 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonEventBridgeSchemasServiceRolePolicy

AmazonEventBridgeSchemasServiceRolePolicy é uma [política gerenciada da AWS](#) que concede permissões às regras gerenciadas criadas pelo Amazon EventBridge Schemas.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de novembro de 2019, 01:10 UTC
- Horário de edição: 27 de novembro de 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy é uma [política gerenciada da AWS](#): Política para permitir que o AWS FIS gerencie o monitoramento e a seleção de atributos para experimentos.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de dezembro de 2020, 21:18 UTC
- Horário de edição: 25 de outubro de 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events>DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
```

```
    "events:DescribeRule"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Tagging",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmHistory"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeUserResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSubnets",
    "iam:GetUser",
    "iam:GetRole",
    "iam:ListUsers",
    "iam:ListRoles",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "ecs:DescribeClusters",
    "ecs:DescribeTasks",
    "ecs:ListTasks",
    "eks:DescribeNodegroup",
    "eks:DescribeCluster"
  ],
  "Resource" : "*"
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonForecastFullAccess

AmazonForecastFullAccess é uma [política gerenciada da AWS](#) que: dá acesso a todas as ações do Amazon Forecast

### A utilização desta política

Você pode vincular a AmazonForecastFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de janeiro de 2019, 01:52 UTC
- Horário de edição: 18 de janeiro de 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "forecast:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "forecast.amazonaws.com"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFraudDetectorFullAccessPolicy

AmazonFraudDetectorFullAccessPolicy é uma [política gerenciada da AWS](#) que: dá acesso a todas as ações do Amazon Fraud Detector

### A utilização desta política

Você pode vincular a AmazonFraudDetectorFullAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS



- Horário de criação: 03 de dezembro de 2019, 22:46 UTC
- Horário de edição: 03 de dezembro de 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "frauddetector.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFreeRTOSFullAccess

AmazonFreeRTOSFullAccess é uma [política gerenciada da AWS](#): política de acesso total para Amazon FreeRTOS

### A utilização desta política

Você pode vincular a AmazonFreeRTOSFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 15:32 UTC
- Horário de edição: 29 de novembro de 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonFreeRTOSOTAUpdate

AmazonFreeRTOSOTAUpdate é uma [política gerenciada da AWS](#) que: permite que o usuário acesse a atualização OTA do Amazon FreeRTOS

## A utilização desta política

Você pode vincular a AmazonFreeRTOSOTAUpdate aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Hora da criação: 27 de agosto de 2018, 22:43 UTC
- Horário de edição: 18 de dezembro de 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "signer:StartSigningJob",
      "signer:DescribeSigningJob",
      "signer:GetSigningProfile",
      "signer:PutSigningProfile"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucketVersions",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:GetBucketLocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteJob",
      "iot:DescribeJob"
    ],
    "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iot:DeleteStream"
    ],
    "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateStream",
      "iot:CreateJob"
    ],
    "Resource" : "*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFSxConsoleFullAccess

AmazonFSxConsoleFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total ao Amazon FSx e acesso aos serviços relacionados AWS por meio de AWS Management Console.

### Utilização desta política

Você pode vincular a AmazonFSxConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2018, 16:36 UTC
- Horário editado: 10 de janeiro de 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess é uma [política gerenciada pela AWS](#) que: fornece acesso somente leitura ao Amazon FSx e acesso aos serviços relacionados AWS por meio de AWS Management Console.

### Utilização desta política

Você pode vincular a AmazonFSxConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2018, 16:35 UTC
- Horário editado: 10 de janeiro de 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFSxFullAccess

AmazonFSxFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total ao Amazon FSx e acesso aos serviços AWS relacionados.

### Utilização desta política

Você pode vincular a AmazonFSxFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2018, 16:34 UTC
- Horário editado: 10 de janeiro de 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

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

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "FullAccessToFSx",
    "Effect" : "Allow",
    "Action" : [
      "fsx:AssociateFileGateway",
      "fsx:AssociateFileSystemAliases",
      "fsx:CancelDataRepositoryTask",
      "fsx:CopyBackup",
      "fsx:CopySnapshotAndUpdateVolume",
      "fsx>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"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonFSxReadOnlyAccess

AmazonFSxReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon FSx.

## A utilização desta política

Você pode vincular a AmazonFSxReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de novembro de 2018, 16:33 UTC
- Horário de edição: 28 de novembro de 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonFSxServiceRolePolicy

AmazonFSxServiceRolePolicy é uma [política gerenciada AWS](#) que: permite que o Amazon FSx crie e gereencie atributos de AWS em seu nome

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 28 de novembro de 2018, 10:38 UTC
- Horário editado: 10 de janeiro de 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    }
  ],
}
```

```
{
  "Sid" : "TagResourceNetworkInterface",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "AmazonFSx.FileSystemId"
    }
  }
},
{
  "Sid" : "ManageNetworkInterface",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
    }
  }
},
{
  "Sid" : "ManageRouteTable",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateRoute",
    "ec2:ReplaceRoute",
    "ec2>DeleteRoute"
  ],
  "Resource" : [
```

```
    "arn:aws:ec2:*:*:route-table/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
    }
  }
},
{
  "Sid" : "PutCloudWatchLogs",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
},
{
  "Sid" : "ManageAuditLogs",
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
}
]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGlacierFullAccess

AmazonGlacierFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Glacier por meio de AWS Management Console.

## A utilização desta política

Você pode vincular a `AmazonGlacierFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGlacierReadOnlyAccess

AmazonGlacierReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Glacier por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonGlacierReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário de edição: 05 de maio de 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
```

```
    "glacier:GetVaultLock",
    "glacier:GetVaultNotifications",
    "glacier:ListJobs",
    "glacier:ListMultipartUploads",
    "glacier:ListParts",
    "glacier:ListTagsForVault",
    "glacier:ListVaults"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGrafanaAthenaAccess

AmazonGrafanaAthenaAccess é uma [política gerenciada da AWS](#): Essa política concede acesso ao Amazon Athena e às dependências necessárias para permitir a consulta e a gravação de resultados no s3 a partir do plug-in Amazon Athena no Amazon Grafana.

### A utilização desta política

Você pode vincular a AmazonGrafanaAthenaAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 22 de novembro de 2021, 17:11 UTC
- Horário de edição: 22 de novembro de 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchGetPartition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:PutObject",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : [
    "arn:aws:s3::grafana-athena-query-results-*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGrafanaCloudWatchAccess

AmazonGrafanaCloudWatchAccess é uma [política gerenciada da AWS](#): Essa política concede acesso ao Amazon CloudWatch e às dependências necessárias para usar o CloudWatch como fonte de dados dentro do Amazon Managed Grafana.

### A utilização desta política

Você pode vincular a AmazonGrafanaCloudWatchAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de março de 2023, 22:41 UTC
- Horário de edição: 24 de março de 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "cloudwatch:DescribeAlarmHistory",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetInsightRuleReport"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs:GetLogGroupFields",
    "logs:StartQuery",
    "logs:StopQuery",
    "logs:GetQueryResults",
    "logs:GetLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "tag:GetResources",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "oam:ListSinks",
    "oam:ListAttachedLinks"
  ],
  "Resource" : "*"
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGrafanaRedshiftAccess

AmazonGrafanaRedshiftAccess é uma [política gerenciada da AWS](#): Essa política concede acesso com escopo ao Amazon Redshift e às dependências necessárias para usar o plug-in do Amazon Redshift no Amazon Grafana.

### A utilização desta política

Você pode vincular a AmazonGrafanaRedshiftAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 26 de novembro de 2021, 23:15 UTC
- Horário de edição: 26 de novembro de 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
    }
  ]
}
```

```
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy é uma [política gerenciada da AWS](#) que: permite o acesso aos atributos de AWS usados ou gerenciados pelo Amazon Grafana.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de novembro de 2022, 23:10 UTC
- Horário de edição: 08 de novembro de 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```



```
    },
    "Null" : {
      "aws:RequestTag/AmazonGrafanaManaged" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao uso da Amazon GuardDuty.

### Utilização desta política

Você pode vincular a AmazonGuardDutyFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2017, 22:31 UTC
- Horário editado: 16 de novembro de 2023, 23:04 UTC

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

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",

```

```
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IamGetRoleSid1",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGuardDutyMalwareProtectionServiceRolePolicy

AmazonGuardDutyMalwareProtectionServiceRolePolicy é uma [política AWS gerenciada](#) que: a proteção contra GuardDuty malware usa a função vinculada ao serviço (SLR) chamada. AWSServiceRoleForAmazonGuardDutyMalwareProtection Essa função vinculada ao serviço permite que a proteção contra GuardDuty malware realize varreduras sem agente para detectar malware. Ele permite GuardDuty criar instantâneos em sua conta e compartilhar os instantâneos com a conta de GuardDuty serviço para verificar se há malware. Ele avalia esses instantâneos compartilhados e inclui os metadados recuperados da instância do EC2 nas descobertas da Proteção contra Malware. GuardDuty A função AWSServiceRoleForAmazonGuardDutyMalwareProtection vinculada ao serviço confia no serviço malware-protection.guardduty.amazonaws.com para assumir a função.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de julho de 2022, 19:06 UTC
- Horário editado: 25 de janeiro de 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ]
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "CreateSnapshotVolumeConditionalStatement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshot",
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/GuardDutyExcluded" : "true"
      }
    }
  },
  {
    "Sid" : "CreateSnapshotConditionalStatement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "GuardDutyScanId"
      }
    }
  },
  {
    "Sid" : "CreateTagsPermission",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:*/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSnapshot"
      }
    }
  },
  {
    "Sid" : "AddTagsToSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/GuardDutyScanId" : "*"
      }
    }
  },
}
```

```
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "GuardDutyExcluded",
        "GuardDutyFindingDetected"
      ]
    }
  },
  {
    "Sid" : "DeleteAndShareSnapshotPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot",
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/GuardDutyScanId" : "*"
      },
      "Null" : {
        "aws:ResourceTag/GuardDutyExcluded" : "true"
      }
    }
  },
  {
    "Sid" : "PreventPublicAccessToSnapshotPermission",
    "Effect" : "Deny",
    "Action" : [
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:Add/group" : "all"
      }
    }
  },
  {
    "Sid" : "CreateGrantPermission",
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
```

```

    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
},
{
  "Sid" : "ShareSnapshotKMSPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    },
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
},
{
  "Sid" : "DescribeKeyPermission",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "arn:aws:kms:*:*:key/*"
}

```

```
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guarddduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guarddduty/*: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"
        }
      }
    }
  ]
}
```



## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos GuardDuty recursos da Amazon

### Utilização desta política

Você pode vincular a AmazonGuardDutyReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2017, 22:29 UTC
- Horário editado: 16 de novembro de 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "guardduty:Describe*",
      "guardduty:Get*",
      "guardduty:List*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonGuardDutyServiceRolePolicy

AmazonGuardDutyServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso aos AWS recursos usados ou gerenciados pelo Amazon Guard Duty

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 28 de novembro de 2017, 20:12 UTC
- Horário editado: 09 de fevereiro de 2024, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
      ]
    }
  ]
}
```

```

    "s3:GetBucketPublicAccessBlock",
    "s3:GetEncryptionConfiguration",
    "s3:GetBucketTagging",
    "s3:GetAccountPublicAccessBlock",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "lambda:GetFunctionConfiguration",
    "lambda:ListTags",
    "eks:ListClusters",
    "eks:DescribeCluster",
    "ec2:DescribeVpcEndpointServices",
    "ec2: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"  
      ]  
    }  
  }  
} ]  
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonHealthLakeFullAccess

AmazonHealthLakeFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao serviço do Amazon HealthLake.

### A utilização desta política

Você pode vincular a AmazonHealthLakeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de fevereiro de 2021, 01:07 UTC
- Horário de edição: 17 de fevereiro de 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao serviço do Amazon HealthLake.

## A utilização desta política

Você pode vincular a AmazonHealthLakeReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de fevereiro de 2021, 02:43 UTC
- Horário de edição: 17 de fevereiro de 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
    },
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeFullAccess

AmazonHoneycodeFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Honeycode por meio do AWS Management Console e do SDK.

### A utilização desta política

Você pode vincular a AmazonHoneycodeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:28 UTC
- Horário de edição: 24 de junho de 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Honeycode por meio do AWS Management Console e do SDK.

### A utilização desta política

Você pode vincular a AmazonHoneycodeReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:28 UTC
- Horário de edição: 01 de dezembro de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy é uma [política gerenciada da AWS](#) que: é necessária uma função vinculada ao serviço para que o Amazon Honeycode acesse atributos em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de novembro de 2020, 18:03 UTC
- Horário de edição: 18 de novembro de 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Honeycode Team Association por meio do AWS Management Console e do SDK.

### A utilização desta política

Você pode vincular a AmazonHoneycodeTeamAssociationFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:28 UTC
- Horário de edição: 24 de junho de 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeTeamAssociationReadOnlyAccess

AmazonHoneycodeTeamAssociationReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Honeycode Team Association por meio do AWS Management Console e do SDK.

### A utilização desta política

Você pode vincular a AmazonHoneycodeTeamAssociationReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:27 UTC
- Horário de edição: 24 de junho de 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeWorkbookFullAccess

AmazonHoneycodeWorkbookFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Honeycode Workbook por meio do AWS Management Console e do SDK.

## A utilização desta política

Você pode vincular a AmazonHoneycodeWorkbookFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:28 UTC
- Horário de edição: 01 de dezembro de 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonHoneycodeWorkbookReadOnlyAccess

AmazonHoneycodeWorkbookReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Honeycode Workbook por meio do AWS Management Console e do SDK.

### A utilização desta política

Você pode vincular a AmazonHoneycodeWorkbookReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 20:28 UTC
- Horário de edição: 01 de dezembro de 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "honeycode:GetScreenData",
      "honeycode:DescribeTableDataImportJob",
      "honeycode:ListTableColumns",
      "honeycode:ListTableRows",
      "honeycode:ListTables",
      "honeycode:QueryTableRows"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspector2AgentlessServiceRolePolicy

AmazonInspector2AgentlessServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede ao Amazon Inspector acesso aos Serviços da AWS necessário para realizar avaliações de segurança sem agentes

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 20 de novembro de 2023, 15:18 UTC
- Horário editado: 20 de novembro de 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    }
  ]
}
```

```
},
{
  "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ]
},
{
  "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
  "Effect" : "Deny",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
    }
  }
},
{
  "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:TagKeys" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "InspectorScan"
    }
  }
},
{
  "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:CreateAction" : "CreateSnapshots"
    }
  }
},
```

```

    "Null" : {
      "aws:TagKeys" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "InspectorScan"
    }
  }
},
{
  "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteSnapshot",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/InspectorScan" : "*"
    }
  }
},
{
  "Sid" : "DenyKmsDecryptForExcludedKeys",
  "Effect" : "Deny",
  "Action" : "kms:Decrypt",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/InspectorEc2Exclusion" : "true"
    }
  }
},
{
  "Sid" : "DecryptSnapshotBlocksVolContext",
  "Effect" : "Allow",
  "Action" : "kms:Decrypt",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id" : "vol-*"
    }
  }
}

```

```
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspector2FullAccess

AmazonInspector2FullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Inspector e acesso a outros serviços relacionados, como organizações.

### A utilização desta política

Você pode vincular a AmazonInspector2FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 19:10 UTC
- Horário de edição: 03 de agosto de 2023, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "inspector2.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonInspector2ManagedCisPolicy

AmazonInspector2ManagedCisPolicy é uma [política AWS gerenciada](#) que: Essa é uma política gerenciada que o cliente deve anexar às suas funções para se comunicar com o serviço de inspeção para exames do CIS

## Utilização desta política

Você pode vincular a AmazonInspector2ManagedCisPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 24 de janeiro de 2024, 16:31 UTC
- Horário editado: 24 de janeiro de 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspector2ReadOnlyAccess

AmazonInspector2ReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura ao serviço Amazon inspector2 e aos serviços de suporte relevantes

### A utilização desta política

Você pode vincular a AmazonInspector2ReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de janeiro de 2022, 14:45 UTC
- Horário de edição: 22 de setembro de 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspector2ServiceRolePolicy

AmazonInspector2ServiceRolePolicy é uma [política gerenciada pela AWS](#) que: concede ao Amazon Inspector acesso aos Serviços da AWS necessário para realizar avaliações de segurança

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de novembro de 2021, 20:27 UTC
- Horário editado: 22 de janeiro de 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

## Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2: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"
    }
  }
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspectorFullAccess

AmazonInspectorFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Inspector.

### A utilização desta política

Você pode vincular a AmazonInspectorFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de outubro de 2015, 17:08 UTC
- Horário de edição: 21 de dezembro de 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
```

```

    "ec2:DescribeTags",
    "sns:ListTopics",
    "events:DescribeRule",
    "events:ListRuleNamesByTarget"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "inspector.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "inspector.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonInspectorReadOnlyAccess

AmazonInspectorReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Inspector.

## A utilização desta política

Você pode vincular a AmazonInspectorReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de outubro de 2015, 17:08 UTC
- Horário de edição: 01 de outubro de 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",

```

```
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonInspectorServiceRolePolicy

AmazonInspectorServiceRolePolicy é uma [política gerenciada da AWS](#) que: concede ao Amazon Inspector acesso aos Serviços da AWS necessário para realizar avaliações de segurança

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de novembro de 2017, 15:48 UTC
- Horário de edição: 11 de setembro de 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

### Versão da política

Versão da política: v5 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",

```

```
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKendraFullAccess

AmazonKendraFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Kendra por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKendraFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 16:15 UTC
- Horário de edição: 03 de dezembro de 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
```

```

        "kms:ListAliases",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:ListSecrets"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:GetMetricData"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
},
{
    "Effect" : "Allow",
    "Action" : "kendra:*",
    "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKendraReadOnlyAccess

AmazonKendraReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Kendra por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKendraReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 16:13 UTC
- Horário de edição: 27 de maio de 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKeyspacesFullAccess

AmazonKeyspacesFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Keyspaces

### A utilização desta política

Você pode vincular a AmazonKeyspacesFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de abril de 2020, 17:06 UTC
- Horário de edição: 03 de outubro de 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
```

```

    "Action" : [
      "cloudwatch:DeleteAlarms",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ApplicationAutoscalingServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "KeyspacesReplicationServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "Ec2VpcReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource" : "*"
  }
]
}

```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKeyspacesReadOnlyAccess

AmazonKeyspacesReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Keyspaces

### A utilização desta política

Você pode vincular a AmazonKeyspacesReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de abril de 2020, 17:07 UTC
- Horário de edição: 07 de julho de 2022, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "cassandra:Select"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKeyspacesReadOnlyAccess\_v2

AmazonKeyspacesReadOnlyAccess\_v2 é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Keyspaces e serviços AWS relacionados.

### A utilização desta política

Você pode vincular a AmazonKeyspacesReadOnlyAccess\_v2 aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de setembro de 2023, 17:01 UTC
- Horário de edição: 12 de setembro de 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisAnalyticsFullAccess

AmazonKinesisAnalyticsFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Kinesis Analytics por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKinesisAnalyticsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de setembro de 2016, 19:01 UTC
- Horário de edição: 21 de setembro de 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisAnalyticsReadOnly

AmazonKinesisAnalyticsReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Kinesis Analytics por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKinesisAnalyticsReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de setembro de 2016, 18:16 UTC
- Horário de edição: 21 de setembro de 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "logs:GetLogEvents",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListPolicyVersions",
    "iam:ListRoles"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonKinesisFirehoseFullAccess

AmazonKinesisFirehoseFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total a todos os streams de entrega do Amazon Kinesis Firehose.

## A utilização desta política

Você pode vincular a AmazonKinesisFirehoseFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de outubro de 2015, 18:45 UTC
- Horário de edição: 07 de outubro de 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisFirehoseReadOnlyAccess

AmazonKinesisFirehoseReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura a todos os streams de entrega do Amazon Kinesis Firehose.

### A utilização desta política

Você pode vincular a AmazonKinesisFirehoseReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de outubro de 2015, 18:43 UTC
- Horário de edição: 07 de outubro de 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisFullAccess

AmazonKinesisFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total a todos os streams por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKinesisFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisReadOnlyAccess

AmazonKinesisReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura a todos os streams por meio de AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonKinesisReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisVideoStreamsFullAccess

AmazonKinesisVideoStreamsFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Kinesis Video Streams por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKinesisVideoStreamsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2017, 23:27 UTC
- Horário de edição: 01 de dezembro de 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonKinesisVideoStreamsReadOnlyAccess

AmazonKinesisVideoStreamsReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao AWS Kinesis Video Streams por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonKinesisVideoStreamsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2017, 23:14 UTC
- Horário de edição: 01 de dezembro de 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLaunchWizard\_Fullaccess

AmazonLaunchWizard\_Fullaccess é uma [política gerenciada AWS](#): acesso total ao AWS Launch Wizard e a outros serviços necessários.

### A utilização desta política

Você pode vincular a AmazonLaunchWizard\_Fullaccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de agosto de 2020, 17:47 UTC



- Horário de edição: 22 de fevereiro de 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

## Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",

```

```
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AllocateHosts",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:CreateDhcpOptions",
    "ec2:CreateEgressOnlyInternetGateway",
    "ec2:CreateNetworkInterface",
```

```
"ec2:CreateVolume",
"ec2:CreateVpcEndpoint",
"ec2:CreateTags",
"ec2>DeleteTags",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:ModifyVpcAttribute",
"ec2:AssociateDhcpOptions",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVolume",
"ec2>DeleteDhcpOptions",
"ec2>DeleteInternetGateway",
"ec2>DeleteKeyPair",
"ec2>DeleteNatGateway",
"ec2>DeleteSecurityGroup",
"ec2>DeleteVolume",
"ec2>DeleteVpc",
"ec2:DetachInternetGateway",
"ec2:DetachVolume",
"ec2>DeleteSnapshot",
"ec2:AssociateRouteTable",
"ec2:AssociateVpcCidrBlock",
"ec2>DeleteNetworkAcl",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2>DeleteSubnet",
"ec2:DetachNetworkInterface",
"ec2:DisassociateAddress",
"ec2:DisassociateVpcCidrBlock",
"ec2:GetLaunchTemplateData",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolume",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:GetConsoleOutput",
"ec2:GetPasswordData",
"ec2:ReleaseAddress",
"ec2:ReplaceRoute",
```

```

    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem:DeleteFileSystem",
    "elasticfilesystem:DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",
    "cloudformation>DeleteStack"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
    "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",

```

```

    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:AddRoleToInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
    "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
    "arn:aws:iam:*:*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
    "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:CreateOrUpdateTags",
      "logs:CreateLogStream",
      "logs>DeleteLogGroup",
      "logs>DeleteLogStream",
      "logs:DescribeLog*",
      "logs:PutLogEvents",
      "resource-groups:CreateGroup",
      "resource-groups>DeleteGroup",
      "sns:ListSubscriptionsByTopic",
      "sns:Publish",
      "ssm>DeleteDocument",
      "ssm>DeleteParameter*",
      "ssm:DescribeDocument*",
      "ssm:GetDocument",
      "ssm:PutParameter"
    ],
    "Resource" : [
      "arn:aws:resource-groups:*:*:group/LaunchWizard*",
      "arn:aws:sns:*:*:*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
      "arn:aws:ssm:*:*:parameter/LaunchWizard*",
      "arn:aws:ssm:*:*:document/LaunchWizard*",
      "arn:aws:logs:*:*:log-group:*:*:*",
      "arn:aws:logs:*:*:log-group:LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument",
      "ssm:SendCommand"
    ],
    "Resource" : [

```

```

    "arn:aws:ssm:*:*:document/AWS-RunShellScript"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DeleteLogStream",
    "logs:GetLogEvents",
    "logs:PutLogEvents",
    "ssm:AddTagsToResource",
    "ssm:DescribeDocument",
    "ssm:GetDocument",
    "ssm:ListTagsForResource",
    "ssm:RemoveTagsFromResource"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:*:*:*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*",
    "arn:aws:ssm:*:*:parameter/LaunchWizard*",
    "arn:aws:ssm:*:*:document/LaunchWizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:Describe*",
    "cloudformation:DescribeAccountLimits",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:List*",

```

```

    "cloudformation:ValidateTemplate",
    "ds:Describe*",
    "ds:ListAuthorizedApplications",
    "ec2:Describe*",
    "ec2:Get*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:List*",
    "logs:CreateLogGroup",
    "logs:GetLogDelivery",
    "logs:GetLogRecord",
    "logs:ListLogDeliveries",
    "resource-groups:Get*",
    "resource-groups:List*",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListServiceQuotas",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "ssm:CreateDocument",
    "ssm:DescribeAutomation*",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeParameters",
    "ssm:GetAutomationExecution",
    "ssm:GetCommandInvocation",
    "ssm:GetParameter*",
    "ssm:GetConnectionStatus",
    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",

```



```
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "logs:GetLog*",
    "Resource" : [
      "arn:aws:logs:*:*:log-group:*:*:*",
      "arn:aws:logs:*:*:log-group:LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:List*",
      "cloudformation:Describe*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "application-insights.amazonaws.com",
          "events.amazonaws.com",
          "autoscaling.amazonaws.com.cn",
          "events.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "launchwizard:*",
    "Resource" : "*"
  }
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:TagQueue",
      "sqs:GetQueueUrl",
      "sqs:AddPermission",
      "sqs:ListQueues",
      "sqs>DeleteQueue",
      "sqs:GetQueueAttributes",
      "sqs:ListQueueTags",
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "iam:GetInstanceProfile",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "route53:ListHostedZones",
      "ec2:CreateSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress",
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:CreateFileSystem",
      "elasticfilesystem:CreateMountTarget",
      "elasticfilesystem:DescribeMountTargets",
      "elasticfilesystem:DescribeMountTargetSecurityGroups"
    ],
    "Resource" : "*"
  },
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::launchwizard*",
    "arn:aws:s3:::launchwizard*/**",
    "arn:aws:s3:::aws-sap-data-provider/config.properties"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "cloudformation:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3>DeleteBucket",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:LaunchWizard*",
    "arn:aws:s3:::launchwizard*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:DescribeTable",
```

```

    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager>CreateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager>DeleteResourcePolicy",
    "secretsmanager>ListSecretVersionIds",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager>ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm>CreateOpsMetadata"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm>DeleteOpsMetadata",
  "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns>CreateTopic",
    "sns>DeleteTopic",
    "sns:Subscribe",

```

```

    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:UntagResource",
    "fsx:TagResource",
    "fsx>DeleteFileSystem",
    "fsx:ListTagsForResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/Name" : "LaunchWizard*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:CreateFileSystem"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/Name" : [
        "LaunchWizard*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "fsx:DescribeFileSystems"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:CreatePortfolio",

```

```

    "servicecatalog:DescribePortfolio",
    "servicecatalog>CreateConstraint",
    "servicecatalog>CreateProduct",
    "servicecatalog:AssociatePrincipalWithPortfolio",
    "servicecatalog>CreateProvisioningArtifact",
    "servicecatalog:TagResource",
    "servicecatalog:UntagResource"
  ],
  "Resource" : [
    "arn:aws:servicecatalog:*:*:*/*",
    "arn:aws:catalog:*:*:*/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor0",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm>DeleteAssociation"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:TagResource"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLaunchWizardFullAccessV2

AmazonLaunchWizardFullAccessV2 é uma [política gerenciada AWS](#): acesso total ao AWS Launch Wizard e a outros serviços necessários.

### A utilização desta política

Você pode vincular a AmazonLaunchWizardFullAccessV2 aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de setembro de 2023, 17:14 UTC
- Horário de edição: 01 de setembro de 2023, 17:14 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
```



```
"Action" : [
  "s3:ListAllMyBuckets",
  "s3:ListBucket",
  "s3:GetBucketLocation"
],
"Resource" : "*"
},
{
  "Sid" : "KmsActions0",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:List*",
    "cloudwatch:Get*",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2Actions0",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateVpc",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2Actions1",
  "Effect" : "Allow",
  "Action" : [
```

```
"ec2:AllocateAddress",
"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateNetworkInterface",
"ec2:CreateVolume",
"ec2:CreateVpcEndpoint",
"ec2:CreateTags",
"ec2>DeleteTags",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:ModifyVpcAttribute",
"ec2:AssociateDhcpOptions",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVolume",
"ec2>DeleteDhcpOptions",
"ec2>DeleteInternetGateway",
"ec2>DeleteKeyPair",
"ec2>DeleteNatGateway",
"ec2>DeleteSecurityGroup",
"ec2>DeleteVolume",
"ec2>DeleteVpc",
"ec2:DetachInternetGateway",
"ec2:DetachVolume",
"ec2>DeleteSnapshot",
"ec2:AssociateRouteTable",
"ec2:AssociateVpcCidrBlock",
"ec2>DeleteNetworkAcl",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2>DeleteSubnet",
"ec2:DetachNetworkInterface",
"ec2:DisassociateAddress",
"ec2:DisassociateVpcCidrBlock",
"ec2:GetLaunchTemplateData",
```

```

    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVolume",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:GetConsoleOutput",
    "ec2:GetPasswordData",
    "ec2:ReleaseAddress",
    "ec2:ReplaceRoute",
    "ec2:ReplaceRouteTableAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DisassociateRouteTable",
    "ec2:DisassociateSubnetCidrBlock",
    "ec2:ModifyInstancePlacement",
    "ec2>DeletePlacementGroup",
    "ec2>CreatePlacementGroup",
    "elasticfilesystem:DeleteFileSystem",
    "elasticfilesystem:DeleteMountTarget",
    "ds:AddIpRoutes",
    "ds:CreateComputer",
    "ds:CreateMicrosoftAD",
    "ds>DeleteDirectory",
    "servicecatalog:AssociateProductWithPortfolio",
    "cloudformation:GetTemplateSummary",
    "sts:GetCallerIdentity"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudFormationActions0",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStack*",
    "cloudformation:Get*",
    "cloudformation:ListStacks",
    "cloudformation:SignalResource",
    "cloudformation>DeleteStack"
  ],
  "Resource" : [

```

```

        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/**",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/**"
    ]
},
{
    "Sid" : "Ec2Actions2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "StringLike" : {
            "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/**"
        }
    }
},
{
    "Sid" : "IamActions0",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
},
{
    "Sid" : "IamActions1",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam:*:*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
},

```

```

    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com",
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Sid" : "AutoScalingActions0",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:CreateOrUpdateTags",
      "resource-groups:CreateGroup",
      "resource-groups>DeleteGroup",
      "sns:ListSubscriptionsByTopic",
      "sns:Publish",
      "ssm>DeleteDocument",
      "ssm>DeleteParameter*",
      "ssm:DescribeDocument*",
      "ssm:GetDocument",
      "ssm:PutParameter"
    ],
    "Resource" : [
      "arn:aws:resource-groups:*:*:group/LaunchWizard*",
      "arn:aws:sns:*:*:*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
      "arn:aws:ssm:*:*:parameter/LaunchWizard*",
      "arn:aws:ssm:*:*:document/LaunchWizard*"
    ]
  },
  {
    "Sid" : "SsmActions0",

```

```

    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument",
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ssm:*::document/AWS-RunShellScript"
    ]
  },
  {
    "Sid" : "SsmActions1",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand"
    ],
    "Resource" : [
      "arn:aws:ec2:*::instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*::stack/LaunchWizard-*/*"
      }
    }
  },
  {
    "Sid" : "SsmActions2",
    "Effect" : "Allow",
    "Action" : [
      "ssm:AddTagsToResource",
      "ssm:DescribeDocument",
      "ssm:GetDocument",
      "ssm:ListTagsForResource",
      "ssm:RemoveTagsFromResource"
    ],
    "Resource" : [
      "arn:aws:ssm:*::parameter/LaunchWizard*",
      "arn:aws:ssm:*::document/LaunchWizard*"
    ]
  },
  {
    "Sid" : "SsmActions3",
    "Effect" : "Allow",
    "Action" : [

```

```

    "autoscaling:Describe*",
    "cloudformation:DescribeAccountLimits",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:List*",
    "cloudformation:ValidateTemplate",
    "ds:Describe*",
    "ds:ListAuthorizedApplications",
    "ec2:Describe*",
    "ec2:Get*",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:List*",
    "resource-groups:Get*",
    "resource-groups:List*",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListServiceQuotas",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "ssm:CreateDocument",
    "ssm:DescribeAutomation*",
    "ssm:DescribeInstanceInformation",
    "ssm:DescribeParameters",
    "ssm:GetAutomationExecution",
    "ssm:GetCommandInvocation",
    "ssm:GetParameter*",
    "ssm:GetConnectionStatus",
    "ssm:ListCommand*",
    "ssm:ListDocument*",
    "ssm:ListInstanceAssociations",
    "ssm:SendAutomationSignal",
    "tag:Get*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SsmActions4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution"
  ]
},

```

```

    "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudFormationActions1",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:List*",
      "cloudformation:Describe*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
  },
  {
    "Sid" : "IamActions2",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "autoscaling.amazonaws.com",
          "application-insights.amazonaws.com",
          "events.amazonaws.com",
          "autoscaling.amazonaws.com.cn",
          "events.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Sid" : "LaunchWizardActions0",
    "Effect" : "Allow",
    "Action" : "launchwizard:*",
    "Resource" : "*"
  },
  {
    "Sid" : "SqsActions0",
    "Effect" : "Allow",

```



```

    "Action" : [
      "sqs:TagQueue",
      "sqs:GetQueueUrl",
      "sqs:AddPermission",
      "sqs:ListQueues",
      "sqs>DeleteQueue",
      "sqs:GetQueueAttributes",
      "sqs:ListQueueTags",
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
  },
  {
    "Sid" : "CloudWatchActions1",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "iam:GetInstanceProfile",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
      "arn:aws:iam:*:*:instance-profile/LaunchWizard*"
    ]
  },
  {
    "Sid" : "EfsActions0",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "route53:ListHostedZones",
      "ec2:CreateSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress",
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:CreateFileSystem",
      "elasticfilesystem:CreateMountTarget",
      "elasticfilesystem:DescribeMountTargets",
      "elasticfilesystem:DescribeMountTargetSecurityGroups"
    ],
    "Resource" : "*"
  },
  {

```

```
"Sid" : "S3Actions1",
"Effect" : "Allow",
"Action" : [
  "s3:GetObject",
  "s3:PutObject"
],
"Resource" : [
  "arn:aws:s3:::launchwizard*",
  "arn:aws:s3:::launchwizard*/**",
  "arn:aws:s3:::aws-sap-data-provider/config.properties"
]
},
{
  "Sid" : "CloudFormationActions2",
  "Effect" : "Allow",
  "Action" : "cloudformation:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : "LaunchWizard*"
    }
  }
},
{
  "Sid" : "LambdaActions0",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3>DeleteBucket",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:LaunchWizard*",
    "arn:aws:s3:::launchwizard*"
  ]
},
{
  "Sid" : "DynamodbActions0",
  "Effect" : "Allow",
```

```

    "Action" : [
      "dynamodb:CreateTable",
      "dynamodb:DescribeTable",
      "dynamodb>DeleteTable"
    ],
    "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
  },
  {
    "Sid" : "SecretsManagerActions0",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:TagResource",
      "secretsmanager:UntagResource",
      "secretsmanager:PutResourcePolicy",
      "secretsmanager>DeleteResourcePolicy",
      "secretsmanager:ListSecretVersionIds",
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
  },
  {
    "Sid" : "SecretsManagerActions1",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetRandomPassword",
      "secretsmanager:ListSecrets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SsmActions5",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateOpsMetadata"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SsmActions6",
    "Effect" : "Allow",
    "Action" : "ssm>DeleteOpsMetadata",
    "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
  }

```

```
  },
  {
    "Sid" : "SnsActions0",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns>DeleteTopic",
      "sns:Subscribe",
      "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
  },
  {
    "Sid" : "FsxActions0",
    "Effect" : "Allow",
    "Action" : [
      "fsx:UntagResource",
      "fsx:TagResource",
      "fsx>DeleteFileSystem",
      "fsx:ListTagsForResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/Name" : "LaunchWizard*"
      }
    }
  },
  {
    "Sid" : "FsxActions1",
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateFileSystem"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/Name" : [
          "LaunchWizard*"
        ]
      }
    }
  },
  {
    {
```

```

    "Sid" : "FsxActions2",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ServiceCatalogActions0",
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:CreatePortfolio",
      "servicecatalog:DescribePortfolio",
      "servicecatalog:CreateConstraint",
      "servicecatalog:CreateProduct",
      "servicecatalog:AssociatePrincipalWithPortfolio",
      "servicecatalog:CreateProvisioningArtifact",
      "servicecatalog:TagResource",
      "servicecatalog:UntagResource"
    ],
    "Resource" : [
      "arn:aws:servicecatalog:*:*:*/*",
      "arn:aws:catalog:*:*:*/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SsmActions7",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateAssociation",
      "ssm>DeleteAssociation"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
      "arn:aws:ssm:*:*:association/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  }
}

```

```
    }
  }
},
{
  "Sid" : "EfsActions1",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:UntagResource",
    "elasticfilesystem:TagResource"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
},
{
  "Sid" : "LogsActions0",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs>DeleteLogGroup",
    "logs:DescribeLogStreams",
    "logs:UntagResource",
    "logs:TagResource",
    "logs:CreateLogGroup",
    "logs>DeleteLogStream",
    "logs:PutLogEvents",
    "logs:GetLogEvents",
    "logs:GetLogDelivery",
    "logs:GetLogGroupFields",
    "logs:GetLogRecord",
    "logs:ListLogDeliveries"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:LaunchWizard*",
    "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "launchwizard.amazonaws.com"
    }
  }
}
```

```
  },
  {
    "Sid" : "LogsActions1",
    "Effect" : "Allow",
    "Action" : "logs:DescribeLogGroups",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "FsxActions3",
    "Effect" : "Allow",
    "Action" : [
      "fsx:CreateStorageVirtualMachine",
      "fsx:CreateVolume"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "launchwizard.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "FsxActions4",
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeStorageVirtualMachines",
      "fsx:DescribeVolumes"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "launchwizard.amazonaws.com"
        ]
      }
    }
  }
}
```

```
    ]
  }
}
},
{
  "Sid" : "FsxActions5",
  "Effect" : "Allow",
  "Action" : [
    "fsx:DeleteStorageVirtualMachine",
    "fsx:DeleteVolume"
  ],
  "Resource" : [
    "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
    "arn:aws:fsx:*:*:backup/*",
    "arn:aws:fsx:*:*:volume/*/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "launchwizard.amazonaws.com"
      ]
    }
  }
}
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonLexChannelsAccess

AmazonLexChannelsAccess é uma [política gerenciada AWS](#): essa política permite que os clientes chamem o Lex runtime a partir dos canais

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de janeiro de 2021, 20:12 UTC
- Horário de dição: 13 de janeiro de 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLexFullAccess

AmazonLexFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Lex por meio do AWS Management Console. Também fornece acesso para criar funções vinculadas ao serviço Lex e conceder permissões Lex para invocar um conjunto limitado de funções Lambda.

### Utilização desta política

Você pode vincular a AmazonLexFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de abril de 2017, 23:20 UTC
- Horário editado: 07 de fevereiro de 2024, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
```

```

    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:DescribeAlarmsForMetric",
      "kms:DescribeKey",
      "kms:ListAliases",
      "lambda:GetPolicy",
      "lambda:ListFunctions",
      "lex:*",
      "polly:DescribeVoices",
      "polly:SynthesizeSpeech",
      "kendra:ListIndices",
      "iam:ListRoles",
      "s3:ListAllMyBuckets",
      "logs:DescribeLogGroups",
      "s3:GetBucketLocation"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AmazonLexFullAccessStatement2",
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission",
      "lambda:RemovePermission"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
    "Condition" : {
      "StringEquals" : {
        "lambda:Principal" : "lex.amazonaws.com"
      }
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement3",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [

```

```

        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
},
{
    "Sid" : "AmazonLexFullAccessStatement4",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "lex.amazonaws.com"
        }
    }
},
{
    "Sid" : "AmazonLexFullAccessStatement5",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
    }
},

```

```

{
  "Sid" : "AmazonLexFullAccessStatement6",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "lexv2.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement7",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement8",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```

        "iam:AWSServiceName" : "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"
        ]
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonLexReadOnly

AmazonLexReadOnly é uma [AWS política gerenciada da](#) que: fornece acesso somente leitura ao Amazon Lex.

### A utilização desta política

Você pode vincular a AmazonLexReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de abril de 2017, 23:13 UTC
- Horário de edição: 31 de janeiro de 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

### Versão da política

Versão da política: v4 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
```

```
    "lex:ListBotAliases",
    "lex:ListBotChannels",
    "lex:ListBotRecommendations",
    "lex:ListBotVersions",
    "lex:ListBuiltInIntents",
    "lex:ListBuiltInSlotTypes",
    "lex:ListExports",
    "lex:ListImports",
    "lex:ListIntents",
    "lex:ListRecommendedIntents",
    "lex:ListSlots",
    "lex:ListSlotTypes",
    "lex:ListTagsForResource",
    "lex:SearchAssociatedTranscripts",
    "lex:ListCustomVocabularyItems"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLexReplicationPolicy

AmazonLexReplicationPolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon Lex replique os recursos do Lex em todas as regiões em seu nome.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 31 de janeiro de 2024, 23:29 UTC
- Horário editado: 08 de março de 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex>DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex>DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",

```

```

    "lex:DescribeSlotType",
    "lex:ListSlotTypes",
    "lex:DescribeSlot",
    "lex:ListSlots",
    "lex:DescribeCustomVocabulary",
    "lex:StartImport",
    "lex:DescribeImport",
    "lex:CreateBot",
    "lex:UpdateBot",
    "lex>DeleteBot",
    "lex:CreateBotLocale",
    "lex:UpdateBotLocale",
    "lex>DeleteBotLocale",
    "lex:CreateIntent",
    "lex:UpdateIntent",
    "lex>DeleteIntent",
    "lex:CreateSlotType",
    "lex:UpdateSlotType",
    "lex>DeleteSlotType",
    "lex:CreateSlot",
    "lex:UpdateSlot",
    "lex>DeleteSlot",
    "lex:CreateCustomVocabulary",
    "lex:UpdateCustomVocabulary",
    "lex>DeleteCustomVocabulary",
    "lex>DeleteBotChannel",
    "lex>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"
      }
    }
  }
]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonLexRunBotsOnly

AmazonLexRunBotsOnly é uma [política gerenciada da AWS](#) que: fornece acesso às APIs de conversação do Amazon Lex.

### A utilização desta política

Você pode vincular a AmazonLexRunBotsOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 11 de abril de 2017, 23:06 UTC
- Horário de edição: 18 de agosto de 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex>DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLexV2BotPolicy

AmazonLexV2BotPolicy é uma [política gerenciada da AWS](#) que: fornece aos bots Lex V2 acesso para chamar outros serviços AWS em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de janeiro de 2021, 20:10 UTC
- Horário de edição: 13 de janeiro de 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutEquipmentFullAccess

AmazonLookoutEquipmentFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total às operações do Amazon Lookout for Equipment

### A utilização desta política

Você pode vincular a AmazonLookoutEquipmentFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de abril de 2021, 15:52 UTC
- Horário de edição: 24 de novembro de 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ]
    }
  ]
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutEquipmentReadOnlyAccess

AmazonLookoutEquipmentReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura às operações do Amazon Lookout for Equipment

### A utilização desta política

Você pode vincular a AmazonLookoutEquipmentReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de maio de 2021, 16:47 UTC
- Horário de edição: 10 de novembro de 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutMetricsFullAccess

AmazonLookoutMetricsFullAccess é uma [política gerenciada da AWS](#) que: dá acesso a todas as ações do Amazon Lookout for Metrics

## A utilização desta política

Você pode vincular a AmazonLookoutMetricsFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de maio de 2021, 00:43 UTC
- Horário de edição: 07 de maio de 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutMetricsReadOnlyAccess

AmazonLookoutMetricsReadOnlyAccess é uma [política gerenciada da AWS](#) que: dá acesso a todas as ações somente leitura para o Amazon Lookout for Metrics

### A utilização desta política

Você pode vincular a AmazonLookoutMetricsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de maio de 2021, 00:43 UTC
- Horário de edição: 04 de janeiro de 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonLookoutVisionConsoleFullAccess

AmazonLookoutVisionConsoleFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Lookout for Vision e acesso com escopo às dependências necessárias do serviço e do console.

## A utilização desta política

Você pode vincular a AmazonLookoutVisionConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2021, 19:37 UTC
- Horário de edição: 11 de maio de 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
{
  "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutBucketVersioning",
    "s3:PutLifecycleConfiguration",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketVersioning"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*"
},
{
  "Sid" : "LookoutVisionConsoleS3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject",
    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*/*"
},
{
  "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
```



```
    "Effect" : "Allow",
    "Action" : [
      "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
      "groundtruthlabeling:AssociatePatchToManifestJob",
      "groundtruthlabeling:DescribeConsoleJob"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleDashboardAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleTagSelectorAccess",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetTagKeys",
      "tag:GetTagValues"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:ListAliases"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutVisionConsoleReadOnlyAccess

AmazonLookoutVisionConsoleReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Lookout for Vision e acesso limitado às dependências necessárias do serviço e do console.

### A utilização desta política

Você pode vincular a AmazonLookoutVisionConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2021, 19:32 UTC
- Horário de edição: 09 de dezembro de 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "lookoutvision:DescribeDataset",
    "lookoutvision:DescribeModel",
    "lookoutvision:DescribeProject",
    "lookoutvision:DescribeTrialDetection",
    "lookoutvision:DescribeModelPackagingJob",
    "lookoutvision>ListDatasetEntries",
    "lookoutvision>ListModels",
    "lookoutvision>ListProjects",
    "lookoutvision>ListTagsForResource",
    "lookoutvision>ListTrialDetections",
    "lookoutvision>ListModelPackagingJobs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3>ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::lookoutvision-*/*"
},
{
  "Sid" : "LookoutVisionConsoleDashboardAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Lookout for Vision e acesso limitado às dependências necessárias do serviço e do console.

### A utilização desta política

Você pode vincular a AmazonLookoutVisionFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2021, 19:24 UTC
- Horário de edição: 11 de maio de 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonLookoutVisionReadOnlyAccess

AmazonLookoutVisionReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Lookout for Vision e acesso limitado às dependências necessárias.

### A utilização desta política

Você pode vincular a AmazonLookoutVisionReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2021, 19:11 UTC
- Horário de edição: 09 de dezembro de 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMachineLearningBatchPredictionsAccess

AmazonMachineLearningBatchPredictionsAccess é uma [política gerenciada da AWS](#) que concede aos usuários permissão para solicitar previsões em lote do Amazon Machine Learning.

## A utilização desta política

Você pode vincular a AmazonMachineLearningBatchPredictionsAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de abril de 2015, 17:12 UTC
- Horário de edição: 09 de abril de 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMachineLearningCreateOnlyAccess

AmazonMachineLearningCreateOnlyAccess é uma [política gerenciada da AWS](#) que: Fornece acesso de criação para atributos do Amazon Machine Learning sem previsão.

### A utilização desta política

Você pode vincular a AmazonMachineLearningCreateOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de abril de 2015, 17:18 UTC
- Horário de edição: 29 de junho de 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMachineLearningFullAccess

AmazonMachineLearningFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total para atributos do Amazon Machine Learning.

### A utilização desta política

Você pode vincular a AmazonMachineLearningFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 09 de abril de 2015, 17:25 UTC
- Horário de edição: 09 de abril de 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMachineLearningManageRealTimeEndpointOnlyAccess

AmazonMachineLearningManageRealTimeEndpointOnlyAccess é uma [política gerenciada da AWS](#) que: concede aos usuários permissão para criar e excluir o endpoint em tempo real para os modelos do Amazon Machine Learning.

## A utilização desta política

Você pode vincular a AmazonMachineLearningManageRealTimeEndpointOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de abril de 2015, 17:32 UTC
- Horário de edição: 09 de abril de 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMachineLearningReadOnlyAccess

AmazonMachineLearningReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura para atributos do Amazon Machine Learning.

### A utilização desta política

Você pode vincular a AmazonMachineLearningReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de abril de 2015, 17:40 UTC
- Horário de edição: 09 de abril de 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMachineLearningRealTimePredictionOnlyAccess

AmazonMachineLearningRealTimePredictionOnlyAccess é uma [política gerenciada da AWS](#) que: concede aos usuários permissão para solicitar previsões em tempo real do Amazon Machine Learning.

### A utilização desta política

Você pode vincular a AmazonMachineLearningRealTimePredictionOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 09 de abril de 2015, 17:44 UTC
- Horário de edição: 09 de abril de 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMachineLearningRoleforRedshiftDataSourceV3

AmazonMachineLearningRoleforRedshiftDataSourceV3 é uma [política gerenciada da AWS](#) que: permite que o Machine Learning configure e use seus clusters do Redshift e locais de armazenamento do S3 para a fonte de dados do Redshift.

## A utilização desta política

Você pode vincular a AmazonMachineLearningRoleforRedshiftDataSourceV3 aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de junho de 2020, 18:00 UTC
- Horário de edição: 24 de junho de 2020, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
```

```

    "ec2:RevokeSecurityGroupIngress",
    "redshift:AuthorizeClusterSecurityGroupIngress",
    "redshift:CreateClusterSecurityGroup",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSecurityGroups",
    "redshift:ModifyCluster",
    "redshift:RevokeClusterSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource" : "arn:aws:s3:::amazon-machine-learning*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMacieFullAccess

AmazonMacieFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Macie.

### A utilização desta política

Você pode vincular a AmazonMacieFullAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de agosto de 2017, 14:54 UTC
- Horário de edição: 01 de julho de 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
```

```
    "Action" : "pricing:GetProducts",
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMacieHandshakeRole

AmazonMacieHandshakeRole é uma [política gerenciada da AWS](#) que: Concede permissão para criar a função vinculada ao serviço do Amazon Macie.

### A utilização desta política

Você pode vincular a AmazonMacieHandshakeRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 28 de junho de 2018, 15:46 UTC
- Horário de edição: 28 de junho de 2018, 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMacieReadOnlyAccess

AmazonMacieReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Macie.

### A utilização desta política

Você pode vincular a AmazonMacieReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 15 de junho de 2023, 21:50 UTC
- Horário de edição: 15 de junho de 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMacieServiceRole

AmazonMacieServiceRole é uma [política gerenciada da AWS](#) que: concede ao Macie acesso somente leitura às dependências de atributos de sua conta para permitir a análise dos dados.

## A utilização desta política

Você pode vincular a AmazonMacieServiceRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de agosto de 2017, 14:53 UTC
- Horário editado: 14 de agosto de 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy é uma [política gerenciada da AWS](#): função vinculada ao serviço para a Amazon Macie

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de junho de 2018, 22:17 UTC
- Horário de edição: 19 de maio de 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/maciek/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonManagedBlockchainConsoleFullAccess

AmazonManagedBlockchainConsoleFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Managed Blockchain por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonManagedBlockchainConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de abril de 2019, 21:23 UTC
- Horário de edição: 29 de abril de 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess é uma [política gerenciada da AWS](#) que: fornece acesso total ao Amazon Managed Blockchain.

## A utilização desta política

Você pode vincular a `AmazonManagedBlockchainFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de abril de 2019, 21:39 UTC
- Horário de edição: 29 de abril de 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonManagedBlockchainReadOnlyAccess

AmazonManagedBlockchainReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon Managed Blockchain.

### A utilização desta política

Você pode vincular a AmazonManagedBlockchainReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 30 de abril de 2019, 18:17 UTC
- Horário de edição: 30 de abril de 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon Managed Blockchain

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de janeiro de 2020, 19:51 UTC
- Horário editado: 17 de janeiro de 2020, 19:51 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMCSFullAccess

AmazonMCSFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Managed Apache Cassandra Service

### A utilização desta política

Você pode vincular a AmazonMCSFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 13:45 UTC
- Horário editado: 17 de abril de 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```

    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:RegisterScalableTarget",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling>DeleteScheduledAction",
    "application-autoscaling:DescribeScheduledActions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cassandra:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMCSReadOnlyAccess

AmazonMCSReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Managed Apache Cassandra Service

### A utilização desta política

Você pode vincular a AmazonMCSReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 13:46 UTC
- Horário editado: 17 de abril de 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingActivities",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:DescribeScheduledActions",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMechanicalTurkFullAccess

AmazonMechanicalTurkFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as APIs no Amazon Mechanical Turk.

### A utilização desta política

Você pode vincular a AmazonMechanicalTurkFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de dezembro de 2015, 19:08 UTC
- Horário editado: 11 de dezembro de 2015, 19:08 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMechanicalTurkReadOnly

AmazonMechanicalTurkReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso a APIs somente para leitura no Amazon Mechanical Turk.

## A utilização desta política

Você pode vincular a AmazonMechanicalTurkReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de dezembro de 2015, 19:08 UTC
- Horário editado: 25 de setembro de 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMemoryDBFullAccess

AmazonMemoryDBFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon MemoryDB por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonMemoryDBFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de outubro de 2021, 19:24 UTC
- Horário editado: 08 de outubro de 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMemoryDBReadOnlyAccess

AmazonMemoryDBReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon MemoryDB por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonMemoryDBReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de outubro de 2021, 19:27 UTC
- Horário editado: 08 de outubro de 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonMobileAnalyticsFinancialReportAccess

AmazonMobileAnalyticsFinancialReportAccess é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura a todos os relatórios, incluindo dados financeiros de todos os recursos do aplicativo.

## A utilização desta política

Você pode vincular a AmazonMobileAnalyticsFinancialReportAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}  
 ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total a todos os recursos do aplicativo.

### A utilização desta política

Você pode vincular a AmazonMobileAnalyticsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMobileAnalyticsNon-financialReportAccess

AmazonMobileAnalyticsNon-financialReportAccess é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura a relatórios não financeiros para todos os recursos do aplicativo.

### A utilização desta política

Você pode vincular a AmazonMobileAnalyticsNon-financialReportAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMobileAnalyticsWriteOnlyAccess

`AmazonMobileAnalyticsWriteOnlyAccess` é uma [política AWS gerenciada](#) que: fornece acesso somente de gravação para colocar dados de eventos para todos os recursos do aplicativo. (Recomendado para integração com SDK)

## A utilização desta política

Você pode vincular a `AmazonMobileAnalyticsWriteOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMonitronFullAccess

AmazonMonitronFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total para gerenciar o Amazon Monitron

### A utilização desta política

Você pode vincular a AmazonMonitronFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de dezembro de 2020, 22:40 UTC
- Horário editado: 08 de junho de 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "monitron:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListKeys",
    "kms:DescribeKey",
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : [
        "monitron.*.amazonaws.com"
      ]
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
{
  "Sid" : "AWSSSOPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "ds:DescribeDirectories",
    "ds:DescribeTrusts"
  ],
  "Resource" : "*"
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMQApiFullAccess

AmazonMQApiFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AmazonMQ por meio de nossa API/SDK.

### A utilização desta política

Você pode vincular a AmazonMQApiFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de dezembro de 2018, 20:31 UTC
- Horário editado: 04 de novembro de 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
    ]
  },
  {
    "Action" : "iam:CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "mq.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMQApiReadOnlyAccess

AmazonMQApiReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AmazonMQ por meio de nossa API/SDK.

### A utilização desta política

Você pode vincular a AmazonMQApiReadOnlyAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de dezembro de 2018, 20:31 UTC
- Horário editado: 18 de dezembro de 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMQFullAccess

AmazonMQFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AmazonMQ por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonMQFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de novembro de 2017, 15:28 UTC
- Horário editado: 04 de novembro de 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",

```

```

    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DetachNetworkInterface",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:CreateSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
  ]
},
{
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "mq.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMQReadOnlyAccess

AmazonMQReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon EFS por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonMQReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de novembro de 2017, 15:30 UTC
- Horário editado: 28 de novembro de 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

```
    "mq:List*",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função vinculada ao serviço para AWS Amazon MQ

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora da criação: 04 de novembro de 2020, 16:07 UTC
- Horário editado: 04 de novembro de 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AMQManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups",
      "logs:CreateLogStream",
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao Amazon MSK Connect

### A utilização desta política

Você pode vincular a AmazonMSKConnectReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de setembro de 2021, 10:18 UTC
- Horário editado: 18 de outubro de 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Action" : [
      "kafkaconnect:ListConnectors",
      "kafkaconnect:ListCustomPlugins",
      "kafkaconnect:ListWorkerConfigurations"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kafkaconnect:DescribeConnector"
    ],
    "Resource" : [
      "arn:aws:kafkaconnect:*:*:connector/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kafkaconnect:DescribeCustomPlugin"
    ],
    "Resource" : [
      "arn:aws:kafkaconnect:*:*:custom-plugin/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kafkaconnect:DescribeWorkerConfiguration"
    ],
    "Resource" : [
      "arn:aws:kafkaconnect:*:*:worker-configuration/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMSKFullAccess

AmazonMSKFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon MSK e outras permissões necessárias para suas dependências.

### A utilização desta política

Você pode vincular a AmazonMSKFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de janeiro de 2019, 22:07 UTC
- Horário editado: 18 de outubro de 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcAttribute",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:ListLogDeliveries",
    "logs:PutResourcePolicy",
    "logs:DescribeResourcePolicies",
    "logs:DescribeLogGroups",
    "S3:GetBucketPolicy",
    "firehose:TagDeliveryStream"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:vpc/*",
    "arn:*:ec2:*:*:subnet/*",
    "arn:*:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AWSMSKManaged" : "true"
    },
    "StringLike" : {
      "aws:RequestTag/ClusterArn" : "*"
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSMSKManaged" : "true"
      },
      "StringLike" : {
        "ec2:ResourceTag/ClusterArn" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "kafka.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/AWSServiceRoleForKafka*",
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "kafka.amazonaws.com"
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao Amazon MSK

### A utilização desta política

Você pode vincular a AmazonMSKReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 14 de janeiro de 2019, 22:28 UTC
- Horário editado: 14 de janeiro de 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonMWAAServiceRolePolicy

AmazonMWAAServiceRolePolicy é uma [política AWS gerenciada](#) que: A função vinculada ao serviço usada pelo Amazon Managed Workflows para o Apache Airflow.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de novembro de 2020, 14:13 UTC
- Horário editado: 17 de novembro de 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AttachNetworkInterface",
      "ec2:CreateNetworkInterface",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeVpcs",
      "ec2:DetachNetworkInterface"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "AmazonMWAAManaged"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint",
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonMWAAManaged" : false
      }
    }
  }
},
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "AmazonMWAAManaged"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricData",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/MWAA"
      ]
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker é uma [política AWS gerenciada](#) que: Essa política concede acesso aos recursos necessários aos funcionários do Nimble Studio Launch Profile. Anexe essa política às instâncias do EC2 criadas pelo Nimble Studio Builder.

### A utilização desta política

Você pode vincular a AmazonNimbleStudio-LaunchProfileWorker aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de abril de 2021, 04:47 UTC
- Horário editado: 28 de abril de 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
```

```
    "fsx:DescribeFileSystems",
    "ds:DescribeDirectories"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "nimble.amazonaws.com"
    }
  },
  "Sid" : "GetLaunchProfileInitializationDependencies"
}
],
"Version" : "2012-10-17"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin é uma [política AWS gerenciada](#) que: Essa política concede acesso aos recursos do Amazon Nimble Studio associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços. Anexe essa política à função de administrador associada ao seu estúdio.

### A utilização desta política

Você pode vincular a AmazonNimbleStudio-StudioAdmin aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 28 de abril de 2021, 04:47 UTC
- Horário editado: 22 de setembro de 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble>DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
      ]
    }
  ]
}
```

```

    "nimble:PutStudioLogEvents",
    "nimble:ListLaunchProfiles",
    "nimble:GetLaunchProfile",
    "nimble:GetLaunchProfileMember",
    "nimble:ListLaunchProfileMembers",
    "nimble:PutLaunchProfileMembers",
    "nimble:UpdateLaunchProfileMember",
    "nimble>DeleteLaunchProfileMember"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers",
    "identitystore:DescribeUser",
    "identitystore:ListUsers"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ds:CreateComputer",
    "ds:DescribeDirectories",
    "ec2:DescribeSubnets",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2>DeleteNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:DescribeSecurityGroups",
    "fsx:DescribeFileSystems"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "nimble.amazonaws.com"
    }
  }
}

```

```
    }  
  }  
],  
"Version" : "2012-10-17"  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonNimbleStudio-StudioUser

AmazonNimbleStudio-StudioUser é uma [política AWS gerenciada](#) que: Essa política concede acesso aos recursos do Amazon Nimble Studio associados ao usuário do estúdio e aos recursos relacionados do estúdio em outros serviços. Anexe essa política à função de usuário associada ao seu estúdio.

## A utilização desta política

Você pode vincular a AmazonNimbleStudio-StudioUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de abril de 2021, 04:48 UTC
- Horário editado: 22 de setembro de 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```

{
  "Effect" : "Allow",
  "Action" : [
    "nimble:ListLaunchProfiles"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "nimble:requesterPrincipalId" : "${nimble:principalId}"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "nimble:ListStudioMembers",
    "nimble:GetStudioMember",
    "nimble:ListEulas",
    "nimble:ListEulaAcceptances",
    "nimble:GetFeatureMap",
    "nimble:PutStudioLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "nimble>DeleteStreamingSession",
    "nimble:GetStreamingSession",
    "nimble:StartStreamingSession",
    "nimble:StopStreamingSession",
    "nimble>CreateStreamingSessionStream",
    "nimble:GetStreamingSessionStream",
    "nimble:ListStreamingSessions",
    "nimble:ListStreamingSessionBackups",
    "nimble:GetStreamingSessionBackup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
    }
  }
}
}

```



```
],  
  "Version" : "2012-10-17"  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOmicsFullAccess

AmazonOmicsFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao Amazon Omics e a outros itens necessários Serviços da AWS. Essa política permite que o usuário visualize e aceite convites de compartilhamento de RAM para acessar recursos fora do usuário. Conta da AWS

## A utilização desta política

Você pode vincular a AmazonOmicsFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de fevereiro de 2023, 00:59 UTC
- Horário editado: 24 de fevereiro de 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOmicsReadOnlyAccess

AmazonOmicsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Omics

### A utilização desta política

Você pode vincular a AmazonOmicsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2022, 04:17 UTC
- Horário editado: 29 de novembro de 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
        "omics:Get*",
        "omics:List*"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOneEnterpriseFullAccess

AmazonOneEnterpriseFullAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões administrativas que permitem acesso a todos os recursos e operações do Amazon One Enterprise.

### Utilização desta política

Você pode vincular a AmazonOneEnterpriseFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2023, 04:58 UTC
- Horário editado: 28 de novembro de 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOneEnterpriseInstallerAccess

AmazonOneEnterpriseInstallerAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões limitadas de leitura e gravação que permitem a instalação e ativação do dispositivo.

## Utilização desta política

Você pode vincular a `AmazonOneEnterpriseInstallerAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2023, 05:00 UTC
- Horário editado: 28 de novembro de 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOneEnterpriseReadOnlyAccess

AmazonOneEnterpriseReadOnlyAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões somente de leitura para todos os recursos e operações do Amazon One Enterprise.

### Utilização desta política

Você pode vincular a AmazonOneEnterpriseReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2023, 04:59 UTC
- Horário editado: 28 de novembro de 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchDashboardsServiceRolePolicy

AmazonOpenSearchDashboardsServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso ao Amazon OpenSearch Dashboards Service para acessar outros AWS serviços, como CloudWatch em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.



## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 22 de dezembro de 2023, 19:38 UTC
- Horário editado: 22 de dezembro de 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchIngestionFullAccess

AmazonOpenSearchIngestionFullAccess é uma [política AWS gerenciada](#) que: Permite que o Amazon OpenSearch Ingestion acesse outros AWS serviços em seu nome.

### A utilização desta política

Você pode vincular a AmazonOpenSearchIngestionFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de abril de 2023, 18:11 UTC
- Horário editado: 26 de abril de 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis>DeletePipeline",
```

```

    "osis:StartPipeline",
    "osis:StopPipeline",
    "osis:ListPipelines",
    "osis:GetPipeline",
    "osis:GetPipelineChangeProgress",
    "osis:ValidatePipeline",
    "osis:GetPipelineBlueprint",
    "osis:ListPipelineBlueprints",
    "osis:TagResource",
    "osis:UntagResource",
    "osis:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "osis.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchIngestionReadOnlyAccess

AmazonOpenSearchIngestionReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon OpenSearch Ingestion Service

## A utilização desta política

Você pode vincular a `AmazonOpenSearchIngestionReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de abril de 2023, 18:09 UTC
- Horário editado: 26 de abril de 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchIngestionServiceRolePolicy

AmazonOpenSearchIngestionServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon OpenSearch Ingestion Service acesse outros AWS serviços em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de novembro de 2022, 16:49 UTC
- Horário editado: 18 de novembro de 2022, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVpcEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/OSISManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteVpcEndpoints"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/OSISManaged" : "true"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/OSIS"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchServerlessServiceRolePolicy

AmazonOpenSearchServerlessServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon OpenSearch Serverless acesse outros AWS serviços, como as APIs do CloudWatch, em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de novembro de 2022, 19:50 UTC
- Horário editado: 24 de novembro de 2022, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess é uma [política AWS gerenciada](#) que: Fornece acesso ao serviço de configuração do Amazon Cognito.

### A utilização desta política

Você pode vincular a AmazonOpenSearchServiceCognitoAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de setembro de 2021, 06:31 UTC
- Horário editado: 20 de dezembro de 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Action" : [
      "cognito-idp:DescribeUserPool",
      "cognito-idp:CreateUserPoolClient",
      "cognito-idp>DeleteUserPoolClient",
      "cognito-idp:UpdateUserPoolClient",
      "cognito-idp:DescribeUserPoolClient",
      "cognito-idp:AdminInitiateAuth",
      "cognito-idp:AdminUserGlobalSignOut",
      "cognito-idp:ListUserPoolClients",
      "cognito-identity:DescribeIdentityPool",
      "cognito-identity:UpdateIdentityPool",
      "cognito-identity:GetIdentityPoolRoles"
    ],
    "Resource" : [
      "arn:aws:cognito-identity:*:*:identitypool/*",
      "arn:aws:cognito-idp:*:*:userpool/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "cognito-identity.amazonaws.com",
          "cognito-identity-us-gov.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "cognito-identity:SetIdentityPoolRoles",
    "Resource" : "*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchServiceFullAccess

AmazonOpenSearchServiceFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço de configuração do Amazon OpenSearch Service.

### A utilização desta política

Você pode vincular a AmazonOpenSearchServiceFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de setembro de 2021, 05:33 UTC
- Horário editado: 08 de setembro de 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "es:*"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchServiceReadOnlyAccess

AmazonOpenSearchServiceReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao serviço de configuração do Amazon OpenSearch Service.

### A utilização desta política

Você pode vincular a AmazonOpenSearchServiceReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de setembro de 2021, 05:38 UTC
- Horário editado: 08 de setembro de 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonOpenSearchServiceRolePolicy

AmazonOpenSearchServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon OpenSearch Service acesse outros AWS serviços, como APIs de rede do EC2 em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de agosto de 2021, 09:27 UTC
- Horário editado: 23 de outubro de 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "Stmt1480452973144",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ]
  },
  {
    "Sid" : "Stmt1480452973165",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Sid" : "Stmt1480452973149",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignIpv6Addresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*"
  },
  {
    "Sid" : "Stmt1480452973150",
    "Effect" : "Allow",
    "Action" : [
      "ec2:UnAssignIpv6Addresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*"
  },
  {
    "Sid" : "Stmt1480452973154",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSecurityGroups"
    ],
  },
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "Stmt1480452973164",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Stmt1480452973174",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Stmt1480452973184",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddListenerCertificates",
      "elasticloadbalancing:RemoveListenerCertificates"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:listener/*"
    ]
  },
  {
    "Sid" : "Stmt1480452973194",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ]
  },
  {
    "Sid" : "Stmt1480452973195",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeTags"
    ]
  }
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Stmt1480452973196",
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Stmt1480452973197",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/ES"
      }
    }
  },
  {
    "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"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPersonalizeFullAccess

AmazonPersonalizeFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Personalize por meio do SDKAWS Management Console. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, CloudWatch).

### A utilização desta política

Você pode vincular a AmazonPersonalizeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 04 de dezembro de 2018, 22:24 UTC
- Horário editado: 30 de maio de 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "personalize:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3::*Personalize*",
      "arn:aws:s3::*personalize*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "personalize.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPollyFullAccess

AmazonPollyFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total aos serviços e recursos do Amazon Polly.

### A utilização desta política

Você pode vincular a AmazonPollyFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2016, 18:59 UTC
- Horário editado: 30 de novembro de 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPollyReadOnlyAccess

AmazonPollyReadOnlyAccess é uma [política gerenciada da AWS](#) que: Concede acesso somente de leitura aos recursos do Amazon Polly.

### A utilização desta política

Você pode vincular a AmazonPollyReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2016, 18:59 UTC
- Horário editado: 17 de julho de 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonPrometheusConsoleFullAccess

AmazonPrometheusConsoleFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total aos recursos AWS gerenciados do Prometheus no console AWS

## A utilização desta política

Você pode vincular a AmazonPrometheusConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 18:11 UTC
- Horário editado: 24 de outubro de 2022, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



```
"Effect" : "Allow",
"Action" : [
  "aps:CreateWorkspace",
  "aps:DescribeWorkspace",
  "aps:UpdateWorkspaceAlias",
  "aps>DeleteWorkspace",
  "aps>ListWorkspaces",
  "aps:DescribeAlertManagerDefinition",
  "aps:DescribeRuleGroupsNamespace",
  "aps>CreateAlertManagerDefinition",
  "aps>CreateRuleGroupsNamespace",
  "aps>DeleteAlertManagerDefinition",
  "aps>DeleteRuleGroupsNamespace",
  "aps>ListRuleGroupsNamespaces",
  "aps:PutAlertManagerDefinition",
  "aps:PutRuleGroupsNamespace",
  "aps:TagResource",
  "aps:UntagResource",
  "aps>CreateLoggingConfiguration",
  "aps:UpdateLoggingConfiguration",
  "aps>DeleteLoggingConfiguration",
  "aps:DescribeLoggingConfiguration"
],
"Resource" : "*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPrometheusFullAccess

AmazonPrometheusFullAccess é uma [política gerenciada pela AWS](#) que: Concede acesso total aos recursos AWS gerenciados do Prometheus

## Utilização desta política

Você pode vincular a `AmazonPrometheusFullAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 15 de dezembro de 2020, 18:10 UTC
- Horário editado: 26 de novembro de 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ]
    }
  ]
}
```

```
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "aps.amazonaws.com"
        ]
      }
    },
    "Resource" : "*"
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPrometheusQueryAccess

AmazonPrometheusQueryAccess é uma [política AWS gerenciada](#) que: Concede acesso para executar consultas nos recursos AWS gerenciados do Prometheus

## A utilização desta política

Você pode vincular a `AmazonPrometheusQueryAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de dezembro de 2020, 01:02 UTC
- Horário editado: 19 de dezembro de 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPrometheusRemoteWriteAccess

AmazonPrometheusRemoteWriteAccess é uma [política AWS gerenciada](#) que: Concede acesso somente de gravação aos espaços de trabalho AWS gerenciados do Prometheus

### A utilização desta política

Você pode vincular a AmazonPrometheusRemoteWriteAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de dezembro de 2020, 01:04 UTC
- Horário editado: 19 de dezembro de 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [  
  {  
    "Action" : [  
      "aps:RemoteWrite"  
    ],  
    "Effect" : "Allow",  
    "Resource" : "*"   
  }  
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonPrometheusScrapperServiceRolePolicy

AmazonPrometheusScrapperServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS recursos gerenciados ou usados pelo Amazon Managed Service for Prometheus Collector

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2023, 14:19 UTC
- Horário editado: 26 de novembro de 2023, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid" : "TagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:*: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:*:eks:*:*:cluster/*"
  },
  {
    "Sid" : "APSWriting",
    "Effect" : "Allow",
    "Action" : "aps:RemoteWrite",
    "Resource" : "arn:*:aps:*:*:workspace/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
}

```



```
}  
  }  
    }  
  ]  
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonQFullAccess

AmazonQFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total para permitir interações com o Amazon Q

### Utilização desta política

Você pode vincular a AmazonQFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 28 de novembro de 2023, 16:00 UTC
- Horário editado: 28 de novembro de 2023, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonQLDBConsoleFullAccess

AmazonQLDBConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon QLDB por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonQLDBConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de setembro de 2019, 18:24 UTC

- Horário editado: 04 de novembro de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb>DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",

```

```

    "qldb:InsertSampleData",
    "qldb:PartiQLCreateTable",
    "qldb:PartiQLCreateIndex",
    "qldb:PartiQLDropTable",
    "qldb:PartiQLDropIndex",
    "qldb:PartiQLUndropTable",
    "qldb:PartiQLDelete",
    "qldb:PartiQLInsert",
    "qldb:PartiQLUpdate",
    "qldb:PartiQLSelect",
    "qldb:PartiQLHistoryFunction",
    "qldb:PartiQLRedact"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "dbqms:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesis:ListStreams",
    "kinesis:DescribeStream"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "qldb.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonQLDBFullAccess

AmazonQLDBFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon QLDB por meio da API do serviço.

### A utilização desta política

Você pode vincular a AmazonQLDBFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de setembro de 2019, 18:23 UTC
- Horário editado: 04 de novembro de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

{
  "Effect" : "Allow",
  "Action" : [
    "qldb:CreateLedger",
    "qldb:UpdateLedger",
    "qldb:UpdateLedgerPermissionsMode",
    "qldb>DeleteLedger",
    "qldb:ListLedgers",
    "qldb:DescribeLedger",
    "qldb:ExportJournalToS3",
    "qldb:ListJournalS3Exports",
    "qldb:ListJournalS3ExportsForLedger",
    "qldb:DescribeJournalS3Export",
    "qldb:CancelJournalKinesisStream",
    "qldb:DescribeJournalKinesisStream",
    "qldb:ListJournalKinesisStreamsForLedger",
    "qldb:StreamJournalToKinesis",
    "qldb:GetDigest",
    "qldb:GetRevision",
    "qldb:GetBlock",
    "qldb:TagResource",
    "qldb:UntagResource",
    "qldb:ListTagsForResource",
    "qldb:SendCommand",
    "qldb:PartiQLCreateTable",
    "qldb:PartiQLCreateIndex",
    "qldb:PartiQLDropTable",
    "qldb:PartiQLDropIndex",
    "qldb:PartiQLUndropTable",
    "qldb:PartiQLDelete",
    "qldb:PartiQLInsert",
    "qldb:PartiQLUpdate",
    "qldb:PartiQLSelect",
    "qldb:PartiQLHistoryFunction",
    "qldb:PartiQLRedact"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {

```

```
        "iam:PassedToService" : "qldb.amazonaws.com"
    }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonQLDBReadOnly

AmazonQLDBReadOnly é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon QLDB.

### A utilização desta política

Você pode vincular a AmazonQLDBReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de setembro de 2019, 18:19 UTC
- Horário editado: 02 de julho de 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonRDSBetaServiceRolePolicy

AmazonRDSBetaServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon RDS gerencie AWS recursos em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de maio de 2018, 19:41 UTC
- Horário editado: 14 de dezembro de 2022, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
```

```

    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteCoipPoolPermission",
    "ec2>DeleteLocalGatewayRouteTablePermission",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVpcEndpoint",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
    }
  }
}
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon RDS Custom execute várias ações de automação e tarefas de gerenciamento de banco de dados por meio de um perfil de instância do EC2.

## Utilização desta política

Você pode vincular a AmazonRDSCustomInstanceProfileRolePolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 27 de fevereiro de 2024, 17:42 UTC
- Horário editado: 27 de fevereiro de 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "ssmAgentPermission2",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetManifest",
      "ssm:PutConfigurePackageResult"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ssmAgentPermission3",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument",
      "ssm:DescribeDocument"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/*"
  },
  {
    "Sid" : "ssmAgentPermission4",
    "Effect" : "Allow",
    "Action" : [
      "ssmmessages:CreateControlChannel",
      "ssmmessages:OpenControlChannel"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ssmAgentPermission5",
    "Effect" : "Allow",
    "Action" : [
      "ec2messages:AcknowledgeMessage",
      "ec2messages>DeleteMessage",
      "ec2messages:FailMessage",
      "ec2messages:GetEndpoint",
```

```
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
},
{
  "Sid" : "createEc2SnapshotPermission1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createEc2SnapshotPermission2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
},
{
  "Sid" : "createEc2SnapshotPermission3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "createTagForEc2SnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ],
      "ec2:CreateAction" : [
        "CreateSnapshot",
        "CreateSnapshots"
      ]
    }
  }
},
{
  "Sid" : "rdsCustomS3ObjectPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:putObject",
    "s3:getObject",
    "s3:getObjectVersion",
```



```

    "s3:AbortMultipartUpload",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : [
    "arn:aws:s3::do-not-delete-rds-custom-*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "rdsCustomS3BucketPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucketVersions",
    "s3:ListBucketMultipartUploads"
  ],
  "Resource" : [
    "arn:aws:s3::do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "readSecretsFromCpPermission",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
  ],
  "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"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AmazonRDSCustomPreviewServiceRolePolicy

AmazonRDSCustomPreviewServiceRolePolicy é uma [política AWS gerenciada](#) que: Amazon RDS Custom Preview Service Role Policy

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de outubro de 2021, 21:44 UTC
- Horário editado: 20 de setembro de 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
```

```

    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVolumes",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DescribeImages",
    "ec2:DescribeVpcs",
    "ec2:RegisterImage",
    "ec2:DeregisterImage",
    "ec2:DescribeTags",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVolumesModifications",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:SearchTransitGatewayMulticastGroups",
    "ec2:GetTransitGatewayMulticastDomainAssociations",
    "ec2:DescribeTransitGatewayMulticastDomains",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRouteTables"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ecc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation",
    "ec2:TerminateInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:RebootInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}

```

```
    ]
  }
}
},
{
  "Sid" : "ecc1scoping",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
},
```

```
{
  "Sid" : "ecc1scoping3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances1",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:image/*",
```



```

    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
    "arn:aws:ec2:*:*:placement-group/*"
  ]
},
{
  "Sid" : "eccRunInstances3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:snapshot/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac",
        "custom-oracle"
      ]
    }
  }
},
{
  "Sid" : "RequireImdsV2",
  "Effect" : "Deny",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringNotEquals" : {
      "ec2:MetadataHttpTokens" : "required"
    },
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances3keyPair1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",

```

```

    "ec2:DeleteKeyPair"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
  ],
  "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" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon RDS Custom gerencie AWS recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de outubro de 2021, 21:39 UTC
- Horário editado: 20 de setembro de 2023, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
  ],
}
```

```

    "Sid" : "ecc2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation",
      "ec2:TerminateInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:RebootInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ecc1scoping",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ecc1scoping2",
    "Effect" : "Allow",

```

```

    "Action" : [
      "ec2:AssociateAddress",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "ecc1scoping3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignPrivateIpAddresses"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances1",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringLike" : {

```



```

        "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
        ]
    }
},
{
    "Sid" : "eccRunInstances2",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group*"
    ]
},
{
    "Sid" : "eccRunInstances3",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:snapshot*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle-rac",
                "custom-oracle"
            ]
        }
    }
},
{
    "Sid" : "RequireImdsV2",
    "Effect" : "Deny",

```

```

    "Action" : "ec2:RunInstances",
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringNotEquals" : {
        "ec2:MetadataHttpTokens" : "required"
      },
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccRunInstances3keyPair1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:DeleteKeyPair"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
    ],
    "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*",
  "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" : "*"
}
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRDSDDataFullAccess

AmazonRDSDDataFullAccess é uma [política AWS gerenciada](#) que: Permite acesso total ao uso das APIs de dados do RDS, das APIs de armazenamento secreto para credenciais do banco de dados do RDS e das APIs de gerenciamento de consultas do console de banco de dados para executar instruções SQL em clusters Aurora Serverless no. Conta da AWS

## A utilização desta política

Você pode vincular a AmazonRDSDDataFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de novembro de 2018, 21:29 UTC
- Horário editado: 20 de novembro de 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDDataFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",

```

```

    "secretsmanager:DeleteSecret",
    "secretsmanager:DescribeSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
},
{
  "Sid" : "RDSDataServiceAccess",
  "Effect" : "Allow",
  "Action" : [
    "dbqms:CreateFavoriteQuery",
    "dbqms:DescribeFavoriteQueries",
    "dbqms:UpdateFavoriteQuery",
    "dbqms>DeleteFavoriteQueries",
    "dbqms:GetQueryString",
    "dbqms:CreateQueryHistory",
    "dbqms:DescribeQueryHistory",
    "dbqms:UpdateQueryHistory",
    "dbqms>DeleteQueryHistory",
    "rds-data:ExecuteSql",
    "rds-data:ExecuteStatement",
    "rds-data:BatchExecuteStatement",
    "rds-data:BeginTransaction",
    "rds-data:CommitTransaction",
    "rds-data:RollbackTransaction",
    "secretsmanager:CreateSecret",
    "secretsmanager:ListSecrets",
    "secretsmanager:GetRandomPassword",
    "tag:GetResources"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonRDSDirectoryServiceAccess

AmazonRDSDirectoryServiceAccess é uma [política AWS gerenciada](#) que: Permite que o RDS acesse o Directory Service Managed AD em nome do cliente para instâncias de banco de dados SQL Server associadas ao domínio.

## A utilização desta política

Você pode vincular a AmazonRDSDirectoryServiceAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 26 de fevereiro de 2016, 02:02 UTC
- Horário editado: 15 de maio de 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
    }
  ]
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSEnhancedMonitoringRole

AmazonRDSEnhancedMonitoringRole é uma [política AWS gerenciada](#) que: Fornece acesso ao Cloudwatch para monitoramento aprimorado do RDS

### A utilização desta política

Você pode vincular a AmazonRDSEnhancedMonitoringRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de novembro de 2015, 19:58 UTC
- Horário editado: 11 de novembro de 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRDSFullAccess

AmazonRDSFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon RDS por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonRDSFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 17 de agosto de 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

## Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",

```

```

    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch>DeleteAlarms",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:GetCoipPoolUsage",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "outposts:GetOutpostInstanceTypes",
    "devops-guru:GetResourceCollection"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "pi:*",
  "Resource" : [
    "arn:aws:pi:*:*:metrics/rds/*",
    "arn:aws:pi:*:*:perf-reports/rds/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : [

```

```
        "rds.amazonaws.com",
        "rds.application-autoscaling.amazonaws.com"
    ]
  }
}
},
{
  "Action" : [
    "devops-guru:SearchInsights",
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [
        "RDS"
      ]
    },
    "Null" : {
      "devops-guru:ServiceNames" : "false"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSPerformanceInsightsFullAccess

AmazonRDSPerformanceInsightsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao RDS Performance Insights por meio do AWS Management Console

## A utilização desta política

Você pode vincular a `AmazonRDSPerformanceInsightsFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de agosto de 2023, 23:41 UTC
- Horário editado: 23 de outubro de 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "pi:CreatePerformanceAnalysisReport",
  "pi:GetPerformanceAnalysisReport",
  "pi:ListPerformanceAnalysisReports",
  "pi>DeletePerformanceAnalysisReport"
],
"Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
},
{
  "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "pi:TagResource",
    "pi:UntagResource",
    "pi:ListTagsForResource"
  ],
  "Resource" : "arn:aws:pi:*:*:*/rds/*"
},
{
  "Sid" : "AmazonRDSDescribeInstanceAccess",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonCloudWatchReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
}
]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSPerformanceInsightsReadOnly

AmazonRDSPerformanceInsightsReadOnly é uma [política AWS gerenciada que: Política](#) somente de leitura para o RDS Performance Insights

### A utilização desta política

Você pode vincular a AmazonRDSPerformanceInsightsReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de abril de 2022, 00:02 UTC
- Horário editado: 23 de outubro de 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "AmazonRDSDescribeDBInstances",
    "Effect" : "Allow",
    "Action" : "rds:DescribeDBInstances",
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRDSDescribeDBClusters",
    "Effect" : "Allow",
    "Action" : "rds:DescribeDBClusters",
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
    "Effect" : "Allow",
    "Action" : "pi:DescribeDimensionKeys",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
    "Effect" : "Allow",
    "Action" : "pi:GetDimensionKeyDetails",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetadata",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:GetResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceDimensions",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
```

```
    "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
    "Effect" : "Allow",
    "Action" : "pi:ListAvailableResourceMetrics",
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
    "Effect" : "Allow",
    "Action" : "pi:GetPerformanceAnalysisReport",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
    "Effect" : "Allow",
    "Action" : "pi:ListPerformanceAnalysisReports",
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
    "Effect" : "Allow",
    "Action" : "pi:ListTagsForResource",
    "Resource" : "arn:aws:pi:*:*:*/rds/*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy é uma [política AWS gerenciada](#) que: Amazon RDS Preview Service Role Policy

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 31 de maio de 2018, 18:02 UTC
- Horário editado: 04 de outubro de 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
```

```

    "ec2:CreateLocalGatewayRouteTablePermission",
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteCoipPoolPermission",
    "ec2>DeleteLocalGatewayRouteTablePermission",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
    }
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon RDS por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a `AmazonRDSReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 14 de abril de 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricData",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "devops-guru:GetResourceCollection"
  ],
  "Resource" : "*"
},
{
  "Action" : [
    "devops-guru:SearchInsights",
    "devops-guru:ListAnomaliesForInsight"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "devops-guru:ServiceNames" : [
        "RDS"
      ]
    },
    "Null" : {
      "devops-guru:ServiceNames" : "false"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRDSServiceRolePolicy

AmazonRDSServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Permite que o Amazon RDS gerencie AWS recursos em seu nome.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de janeiro de 2018, 18:17 UTC
- Horário editado: 19 de janeiro de 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

## Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

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

```
{
  "Sid" : "Ec2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateCoipPoolPermission",
    "ec2:CreateLocalGatewayRouteTablePermission",
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteCoipPoolPermission",
    "ec2>DeleteLocalGatewayRouteTablePermission",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVpcEndpoint",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2>DeleteVpcEndpoints",
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "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"
      }
    }
  }
]
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRedshiftAllCommandsFullAccess

AmazonRedshiftAllCommandsFullAccess é uma [política AWS gerenciada](#) que: Essa política inclui permissões para executar comandos SQL para copiar, carregar, descarregar, consultar e analisar dados no Amazon Redshift. A política também concede permissões para executar instruções selecionadas para serviços relacionados, como Amazon S3, logs do Amazon CloudWatch, Amazon SageMaker ou AWS Glue.

## A utilização desta política

Você pode vincular a `AmazonRedshiftAllCommandsFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de novembro de 2021, 00:48 UTC
- Horário editado: 25 de novembro de 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
```

```

    "sagemaker:StopTrainingJob",
    "sagemaker:DescribeEndpoint",
    "sagemaker:InvokeEndpoint",
    "sagemaker:StopProcessingJob",
    "sagemaker:CreateModel",
    "sagemaker:CreateProcessingJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:model/*redshift*",
    "arn:aws:sagemaker:*:*:training-job/*redshift*",
    "arn:aws:sagemaker:*:*:automl-job/*redshift*",
    "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
    "arn:aws:sagemaker:*:*:processing-job/*redshift*",
    "arn:aws:sagemaker:*:*:transform-job/*redshift*",
    "arn:aws:sagemaker:*:*:endpoint/*redshift*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "SageMaker",
        "/aws/sagemaker/Endpoints",
        "/aws/sagemaker/ProcessingJobs",

```



```

        "/aws/sagemaker/TrainingJobs",
        "/aws/sagemaker/TransformJobs"
    ]
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift/*"
    ]
},
{
    "Effect" : "Allow",

```

```

    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/Redshift" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:Scan",
      "dynamodb:DescribeTable",
      "dynamodb:Getitem"
    ],
    "Resource" : [
      "arn:aws:dynamodb:*:*:table/*redshift*",
      "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:ListInstances"
    ],
    "Resource" : [
      "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:ListInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "elasticmapreduce:ResourceTag/Redshift" : "true"
      }
    }
  }
},
{

```

```

    "Effect" : "Allow",
    "Action" : [
        "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "glue:CreateDatabase",
        "glue>DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue>DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource" : [

```

```
    "arn:aws:secretsmanager:*:*:secret:*redshift*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetRandomPassword",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "redshift.amazonaws.com",
        "glue.amazonaws.com",
        "sagemaker.amazonaws.com",
        "athena.amazonaws.com"
      ]
    }
  }
}
]
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess é uma [política AWS gerenciada](#) do que: Esta política fornece acesso total às APIs de dados do Amazon Redshift. Essa política também concede acesso a outros serviços necessários.

## A utilização desta política

Você pode vincular a AmazonRedshiftDataFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de setembro de 2020, 19:23 UTC
- Horário editado: 07 de abril de 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
```

```

    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
    }
  }
},
{
  "Sid" : "GetCredentialsForAPIUser",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentials",
  "Resource" : [
    "arn:aws:redshift:*:*:dbname:*/*",
    "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
  ]
},
{
  "Sid" : "GetCredentialsWithFederatedIAMCredentials",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentialsWithIAM",
  "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
},
{
  "Sid" : "GetCredentialsForServerless",
  "Effect" : "Allow",
  "Action" : "redshift-serverless:GetCredentials",
  "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/RedshiftDataFullAccess" : "*"
    }
  }
}

```

```
    }
  },
  {
    "Sid" : "DenyCreateAPIUser",
    "Effect" : "Deny",
    "Action" : "redshift:CreateClusterUser",
    "Resource" : [
      "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
    ]
  },
  {
    "Sid" : "ServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "redshift-data.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRedshiftFullAccess

AmazonRedshiftFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Redshift por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a `AmazonRedshiftFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 07 de julho de 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",

```



```

    "cloudwatch:List*",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:EnableAlarmActions",
    "cloudwatch:DisableAlarmActions",
    "tag:GetResources",
    "tag:UntagResources",
    "tag:GetTagValues",
    "tag:GetTagKeys",
    "tag:TagResources"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "redshift.amazonaws.com"
    }
  }
},
{
  "Sid" : "DataAPIPermissions",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:ListStatements",
    "redshift-data:GetStatementResult",
    "redshift-data:DescribeStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerListPermissions",
  "Action" : [
    "secretsmanager:ListSecrets"
  ]
}

```

```
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerCreateGetPermissions",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:TagResource"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRedshiftQueryEditor

AmazonRedshiftQueryEditor é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Redshift Query Editor e às consultas salvas por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a AmazonRedshiftQueryEditor aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de outubro de 2018, 22:50 UTC
- Horário editado: 16 de fevereiro de 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
        "redshift:CreateSavedQuery",
        "redshift>DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
},
{
  "Sid" : "DataAPIPermissions",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "DataAPIIAMSessionPermissionsRestriction",
  "Action" : [
    "redshift-data:GetStatementResult",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:ListStatements"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "SecretsManagerListPermissions",
  "Action" : [
    "secretsmanager:ListSecrets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SecretsManagerCreateGetPermissions",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:TagResource"
  ],
}
```

```
"Effect" : "Allow",
"Resource" : "arn:aws:secretsmanager:*:*:secret:*",
"Condition" : {
  "StringEquals" : {
    "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRedshiftQueryEditorV2FullAccess

AmazonRedshiftQueryEditorV2FullAccess é uma [política gerenciada pela AWS](#) que concede acesso total às operações e aos recursos do Editor de Consultas do Amazon Redshift V2. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift, ler chaves e aliases no AWS KMS e gerenciar os segredos do Query Editor V2 no Secrets Manager. AWS

### Utilização desta política

Você pode vincular a AmazonRedshiftQueryEditorV2FullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 24 de setembro de 2021, 14:06 UTC
- Horário editado: 21 de fevereiro de 2024, 17:20 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
  },
  {
    "Sid" : "ResourceGroupsTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:*",
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRedshiftQueryEditorV2NoSharing

AmazonRedshiftQueryEditorV2NoSharing é uma [política gerenciada pela AWS](#) que: concede a capacidade de trabalhar com o Editor de Consultas do Amazon Redshift V2 sem compartilhar recursos. O principal concedido só pode ler, atualizar e excluir seus próprios recursos, mas não pode compartilhá-los. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no Secrets Manager AWS .

## Utilização desta política

Você pode vincular a `AmazonRedshiftQueryEditorV2NoSharing` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 24 de setembro de 2021, 14:18 UTC
- Horário editado: 21 de fevereiro de 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

## Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
```



```

    "secretsmanager:GetSecretValue",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "ResourceGroupsTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateFolder",
    "sqlworkbench:PutTab",
    "sqlworkbench:BatchDeleteFolder",
    "sqlworkbench>DeleteTab",
    "sqlworkbench:GenerateSession",
    "sqlworkbench:GetAccountInfo",
    "sqlworkbench:GetAccountSettings",
    "sqlworkbench:GetUserInfo",
    "sqlworkbench:GetUserWorkspaceSettings",
    "sqlworkbench:PutUserWorkspaceSettings",
    "sqlworkbench>ListConnections",
    "sqlworkbench>ListFiles",
    "sqlworkbench>ListTabs",
    "sqlworkbench:UpdateFolder",
    "sqlworkbench>ListRedshiftClusters",
    "sqlworkbench:DriverExecute",
  ]
}

```

```

    "sqlworkbench:ListTaggedResources",
    "sqlworkbench:ListQueryExecutionHistory",
    "sqlworkbench:GetQueryExecutionHistory",
    "sqlworkbench:ListNotebooks",
    "sqlworkbench:GetSchemaInference",
    "sqlworkbench:GetAutocompletionMetadata",
    "sqlworkbench:GetAutocompletionResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
    }
  }
}
}

```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRedshiftQueryEditorV2ReadSharing

AmazonRedshiftQueryEditorV2ReadSharing é uma [política gerenciada pela AWS](#) que: concede a capacidade de trabalhar com o Editor de Consultas do Amazon Redshift V2 com compartilhamento limitado de recursos. A entidade principal concedida pode ler, escrever e compartilhar seus próprios recursos. A entidade principal concedida pode ler os recursos compartilhados com sua equipe, mas não pode atualizá-los. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no Secrets Manager AWS .

### Utilização desta política

Você pode vincular a AmazonRedshiftQueryEditorV2ReadSharing aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 24 de setembro de 2021, 14:22 UTC
- Horário editado: 21 de fevereiro de 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
```

```

    "StringEquals" : {
      "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateFolder",
      "sqlworkbench:PutTab",
      "sqlworkbench:BatchDeleteFolder",
      "sqlworkbench>DeleteTab",
      "sqlworkbench:GenerateSession",
      "sqlworkbench:GetAccountInfo",
      "sqlworkbench:GetAccountSettings",
      "sqlworkbench:GetUserInfo",
      "sqlworkbench:GetUserWorkspaceSettings",
      "sqlworkbench:PutUserWorkspaceSettings",
      "sqlworkbench>ListConnections",
      "sqlworkbench>ListFiles",
      "sqlworkbench>ListTabs",
      "sqlworkbench:UpdateFolder",
      "sqlworkbench>ListRedshiftClusters",
      "sqlworkbench:DriverExecute",
      "sqlworkbench>ListTaggedResources",
      "sqlworkbench>ListQueryExecutionHistory",
      "sqlworkbench:GetQueryExecutionHistory",
      "sqlworkbench>ListNotebooks",
      "sqlworkbench:GetSchemaInference",
      "sqlworkbench:GetAutocompletionMetadata",
      "sqlworkbench:GetAutocompletionResource"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sqlworkbench:CreateConnection",
      "sqlworkbench:CreateSavedQuery",
      "sqlworkbench:CreateChart",
      "sqlworkbench:CreateNotebook",
      "sqlworkbench:DuplicateNotebook",

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:DeleteChart",
    "sqlworkbench:DeleteConnection",
    "sqlworkbench:DeleteSavedQuery",
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:UpdateChart",
    "sqlworkbench:UpdateConnection",
    "sqlworkbench:UpdateSavedQuery",
    "sqlworkbench:AssociateConnectionWithTab",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateConnectionWithChart",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:UpdateFileFolder",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:UpdateNotebook",
    "sqlworkbench:DeleteNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookCell",
    "sqlworkbench:DeleteNotebookCell",
    "sqlworkbench:UpdateNotebookCellContent",
    "sqlworkbench:UpdateNotebookCellLayout",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:CreateNotebookVersion",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench:DeleteNotebookVersion",
    "sqlworkbench:RestoreNotebookVersion",
  ]
}

```

```

    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
  "Effect" : "Allow",
  "Action" : "sqlworkbench:TagResource",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "sqlworkbench-resource-owner"
    },
    "StringEquals" : {
      "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
    }
  }
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:GetChart",
    "sqlworkbench:GetConnection",
    "sqlworkbench:GetSavedQuery",
    "sqlworkbench:ListSavedQueryVersions",
    "sqlworkbench:ListTagsForResource",
    "sqlworkbench:AssociateQueryWithTab",
    "sqlworkbench:AssociateNotebookWithTab",
    "sqlworkbench:GetNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:BatchGetNotebookCell",
    "sqlworkbench:ListNotebookVersions",
    "sqlworkbench:GetNotebookVersion",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ExportNotebook"
  ]
}

```



```

    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:TagResource",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "sqlworkbench-team"
      },
      "StringEquals" : {
        "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
        "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
    "Effect" : "Allow",
    "Action" : "sqlworkbench:UntagResource",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "sqlworkbench-team"
      },
      "StringEquals" : {
        "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRedshiftQueryEditorV2ReadWriteSharing

AmazonRedshiftQueryEditorV2ReadWriteSharing é uma [política gerenciada pela AWS](#) que: concede a capacidade de trabalhar com o Editor de Consultas do Amazon Redshift V2 com compartilhamento de recursos. A entidade principal concedida pode ler, escrever e compartilhar seus próprios recursos. A entidade principal concedida pode ler e atualizar os recursos compartilhados com sua equipe. Essa política também concede acesso a outros serviços necessários. Isso inclui permissões para listar os clusters do Amazon Redshift e gerenciar os segredos do Query Editor V2 do principal no Secrets Manager AWS .

### Utilização desta política

Você pode vincular a AmazonRedshiftQueryEditorV2ReadWriteSharing aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 24 de setembro de 2021, 14:25 UTC
- Horário editado: 21 de fevereiro de 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "RedshiftPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters",
      "redshift-serverless:ListNamespaces",
      "redshift-serverless:ListWorkgroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager>DeleteSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "ResourceGroupsTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
    "Effect" : "Allow",

```

```

"Action" : [
  "sqlworkbench:CreateFolder",
  "sqlworkbench:PutTab",
  "sqlworkbench:BatchDeleteFolder",
  "sqlworkbench>DeleteTab",
  "sqlworkbench:GenerateSession",
  "sqlworkbench:GetAccountInfo",
  "sqlworkbench:GetAccountSettings",
  "sqlworkbench:GetUserInfo",
  "sqlworkbench:GetUserWorkspaceSettings",
  "sqlworkbench:PutUserWorkspaceSettings",
  "sqlworkbench:ListConnections",
  "sqlworkbench:ListFiles",
  "sqlworkbench:ListTabs",
  "sqlworkbench:UpdateFolder",
  "sqlworkbench:ListRedshiftClusters",
  "sqlworkbench:DriverExecute",
  "sqlworkbench:ListTaggedResources",
  "sqlworkbench:ListQueryExecutionHistory",
  "sqlworkbench:GetQueryExecutionHistory",
  "sqlworkbench:ListNotebooks",
  "sqlworkbench:GetSchemaInference",
  "sqlworkbench:GetAutocompletionMetadata",
  "sqlworkbench:GetAutocompletionResource"
],
"Resource" : "*"
},
{
  "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:CreateConnection",
    "sqlworkbench:CreateSavedQuery",
    "sqlworkbench:CreateChart",
    "sqlworkbench:CreateNotebook",
    "sqlworkbench:DuplicateNotebook",
    "sqlworkbench:CreateNotebookFromVersion",
    "sqlworkbench:ImportNotebook"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sqlworkbench-resource-owner" : "${aws: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}"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRedshiftReadOnlyAccess

AmazonRedshiftReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Redshift por meio do AWS Management Console

### Utilização desta política

Você pode vincular a AmazonRedshiftReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 08 de fevereiro de 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
```



```
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeInternetGateways",
    "sns:Get*",
    "sns:List*",
    "cloudwatch:Describe*",
    "cloudwatch:List*",
    "cloudwatch:Get*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRedshiftServiceLinkedRolePolicy

AmazonRedshiftServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon Redshift chame AWS serviços em seu nome

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de setembro de 2017, 19:19 UTC

- Horário editado: 15 de março de 2024, 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

## Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
```

```

    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:elastic-ip/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "PublicAccessReleaseEip",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReleaseAddress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:elastic-ip/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/redshift/*"
  ]
},
{
  "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams",

```

```
    "logs:GetLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
  ]
},
{
  "Sid" : "CreateSecurityGroupWithTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "SecurityGroupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:ModifySecurityGroupRules",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/Redshift" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroup",
  "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Sid" : "CreateTagsOnResources",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:vpc/*",
      "arn:aws:ec2:*:*:internet-gateway/*",
      "arn:aws:ec2:*:*:elastic-ip*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateVpc",
          "CreateSecurityGroup",
          "CreateSubnet",
          "CreateInternetGateway",
          "CreateRouteTable",
          "AllocateAddress"
        ]
      }
    }
  },
  {
    "Sid" : "VPCPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeRouteTables"
    ]
  },

```

```

    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Redshift-Serverless",
          "AWS/Redshift"
        ]
      }
    }
  },
  {
    "Sid" : "SecretManager",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue",
      "secretsmanager:UpdateSecret",
      "secretsmanager:UpdateSecretVersionStage",
      "secretsmanager:RotateSecret"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:redshift!*"
    ],
    "Condition" : {
      "StringEquals" : {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "SecretsManagerRandomPassword",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetRandomPassword"
    ]
  }
}

```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IPV6Permissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssignIpv6Addresses",
      "ec2:UnassignIpv6Addresses"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ]
  },
  {
    "Sid" : "ServiceQuotasToCheckCustomerLimits",
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : [
      "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
      "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
    ]
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonRekognitionCustomLabelsFullAccess

AmazonRekognitionCustomLabelsFullAccess é uma [política AWS gerenciada que: Essa política](#) especifica as permissões de reconhecimento e s3 exigidas pelo recurso Amazon Rekognition Custom Labels.

## A utilização desta política

Você pode vincular a `AmazonRekognitionCustomLabelsFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de janeiro de 2020, 19:18 UTC
- Horário editado: 16 de agosto de 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3::*custom-labels*"
    }
  ]
}
```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "rekognition:CreateProject",
      "rekognition:CreateProjectVersion",
      "rekognition:StartProjectVersion",
      "rekognition:StopProjectVersion",
      "rekognition:DescribeProjects",
      "rekognition:DescribeProjectVersions",
      "rekognition:DetectCustomLabels",
      "rekognition>DeleteProject",
      "rekognition>DeleteProjectVersion",
      "rekognition:TagResource",
      "rekognition:UntagResource",
      "rekognition:ListTagsForResource",
      "rekognition:CreateDataset",
      "rekognition:ListDatasetEntries",
      "rekognition:ListDatasetLabels",
      "rekognition:DescribeDataset",
      "rekognition:UpdateDatasetEntries",
      "rekognition:DistributeDatasetEntries",
      "rekognition>DeleteDataset",
      "rekognition:CopyProjectVersion",
      "rekognition:PutProjectPolicy",
      "rekognition:ListProjectPolicies",
      "rekognition>DeleteProjectPolicy"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRekognitionFullAccess

AmazonRekognitionFullAccess é uma [política AWS gerenciada](#) que: Acesso a todas as APIs do Amazon Rekognition

## A utilização desta política

Você pode vincular a AmazonRekognitionFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2016, 14:40 UTC
- Horário editado: 30 de novembro de 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRekognitionReadOnlyAccess

AmazonRekognitionReadOnlyAccess é uma [política gerenciada pela AWS](#) que: Acesso a todas as APIs de reconhecimento de leitura

### Utilização desta política

Você pode vincular a AmazonRekognitionReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 30 de novembro de 2016, 14:58 UTC
- Hora da edição: 08 de novembro de 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```
{
  "Sid" : "AmazonRekognitionReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "rekognition:CompareFaces",
    "rekognition:DetectFaces",
    "rekognition:DetectLabels",
    "rekognition:ListCollections",
    "rekognition:ListFaces",
    "rekognition:SearchFaces",
    "rekognition:SearchFacesByImage",
    "rekognition:DetectText",
    "rekognition:GetCelebrityInfo",
    "rekognition:RecognizeCelebrities",
    "rekognition:DetectModerationLabels",
    "rekognition:GetLabelDetection",
    "rekognition:GetFaceDetection",
    "rekognition:GetContentModeration",
    "rekognition:GetPersonTracking",
    "rekognition:GetCelebrityRecognition",
    "rekognition:GetFaceSearch",
    "rekognition:GetTextDetection",
    "rekognition:GetSegmentDetection",
    "rekognition:DescribeStreamProcessor",
    "rekognition:ListStreamProcessors",
    "rekognition:DescribeProjects",
    "rekognition:DescribeProjectVersions",
    "rekognition:DetectCustomLabels",
    "rekognition:DetectProtectiveEquipment",
    "rekognition:ListTagsForResource",
    "rekognition:ListDatasetEntries",
    "rekognition:ListDatasetLabels",
    "rekognition:DescribeDataset",
    "rekognition:ListProjectPolicies",
    "rekognition:ListUsers",
    "rekognition:SearchUsers",
    "rekognition:SearchUsersByImage",
    "rekognition:GetMediaAnalysisJob",
    "rekognition:ListMediaAnalysisJobs"
  ],
  "Resource" : "*"
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRekognitionServiceRole

AmazonRekognitionServiceRole é uma [política AWS gerenciada](#) que: Permite que o Rekognition chame serviços em seu nome. AWS

### A utilização desta política

Você pode vincular a AmazonRekognitionServiceRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 29 de novembro de 2017, 16:52 UTC
- Horário editado: 29 de novembro de 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRoute53AutoNamingFullAccess

AmazonRoute53AutoNamingFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as ações de nomenclatura automática do Route 53.

## A utilização desta política

Você pode vincular a AmazonRoute53AutoNamingFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de janeiro de 2018, 18:40 UTC
- Horário editado: 18 de janeiro de 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
```

```
    "route53:GetHealthCheck",
    "route53:DeleteHealthCheck",
    "route53:UpdateHealthCheck",
    "ec2:DescribeVpcs",
    "ec2:DescribeRegions",
    "servicediscovery:*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53AutoNamingReadOnlyAccess

AmazonRoute53AutoNamingReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todas as ações de nomenclatura automática do Route 53.

### A utilização desta política

Você pode vincular a AmazonRoute53AutoNamingReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de janeiro de 2018, 03:02 UTC
- Horário editado: 18 de janeiro de 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess é uma [política AWS gerenciada](#) que: Fornece acesso em nível de registrante às ações de nomenclatura automática do Route 53.

## A utilização desta política

Você pode vincular a `AmazonRoute53AutoNamingRegistrantAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de março de 2018, 22:33 UTC
- Horário editado: 12 de março de 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ]
    }
  ]
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53DomainsFullAccess

AmazonRoute53DomainsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as ações de domínios do Route53 e cria zona hospedada para permitir a criação de zonas hospedadas como parte dos registros de domínio.

### A utilização desta política

Você pode vincular a AmazonRoute53DomainsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53DomainsReadOnlyAccess

AmazonRoute53DomainsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso à lista e ações de domínios do Route53.

## A utilização desta política

Você pode vincular a AmazonRoute53DomainsReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53FullAccess

AmazonRoute53FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todo o Amazon Route 53 por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonRoute53FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 20 de dezembro de 2018, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "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"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53ReadOnlyAccess

AmazonRoute53ReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todo o Amazon Route 53 por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonRoute53ReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 15 de novembro de 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryClusterFullAccess

AmazonRoute53RecoveryClusterFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao cluster de recuperação do Amazon Route 53

### A utilização desta política

Você pode vincular a AmazonRoute53RecoveryClusterFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 18:37 UTC
- Horário editado: 18 de agosto de 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryClusterReadOnlyAccess

AmazonRoute53RecoveryClusterReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao cluster de recuperação do Amazon Route 53

### A utilização desta política

Você pode vincular a AmazonRoute53RecoveryClusterReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 17:36 UTC
- Horário editado: 01 de abril de 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryControlConfigFullAccess

AmazonRoute53RecoveryControlConfigFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Route 53 Recovery Control Config

### A utilização desta política

Você pode vincular a AmazonRoute53RecoveryControlConfigFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 17:48 UTC

- Horário editado: 18 de agosto de 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryControlConfigReadOnlyAccess

`AmazonRoute53RecoveryControlConfigReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Route 53 Recovery Control Config

## A utilização desta política

Você pode vincular a `AmazonRoute53RecoveryControlConfigReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 18:01 UTC
- Horário editado: 18 de outubro de 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",

```

```
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryReadinessFullAccess

AmazonRoute53RecoveryReadinessFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à prontidão de recuperação do Amazon Route 53

### A utilização desta política

Você pode vincular a AmazonRoute53RecoveryReadinessFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 16:45 UTC
- Horário editado: 18 de agosto de 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53RecoveryReadinessReadOnlyAccess

AmazonRoute53RecoveryReadinessReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Route 53 Recovery Readiness

## A utilização desta política

Você pode vincular a AmazonRoute53RecoveryReadinessReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de agosto de 2021, 18:11 UTC
- Horário editado: 09 de novembro de 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ],
}
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "route53-recovery-readiness:GetArchitectureRecommendations",
    "route53-recovery-readiness:GetCellReadinessSummary"
  ],
  "Resource" : "arn:aws:route53-recovery-readiness:*:*:*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonRoute53ResolverFullAccess

AmazonRoute53ResolverFullAccess é uma [política AWS gerenciada que: Política](#) de acesso total para o Route 53 Resolver

### A utilização desta política

Você pode vincular a AmazonRoute53ResolverFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de maio de 2019, 18:10 UTC
- Horário editado: 17 de julho de 2020, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess é uma [política AWS gerenciada que: Política](#) somente de leitura para o Route 53 Resolver

## A utilização desta política

Você pode vincular a AmazonRoute53ResolverReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de maio de 2019, 18:11 UTC
- Horário editado: 27 de setembro de 2019, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
```

```
    "ec2:DescribeSubnets"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonS3FullAccess

AmazonS3FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todos os buckets por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonS3FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 27 de setembro de 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy é uma [política AWS gerenciada](#) que: Fornece permissões às funções do AWS Lambda para interagir com o Amazon S3 Object Lambda. Também concede permissões do Lambda para gravar nos logs do CloudWatch.

## A utilização desta política

Você pode vincular a AmazonS3ObjectLambdaExecutionRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 18 de agosto de 2021, 10:07 UTC
- Horário editado: 18 de agosto de 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonS3OutpostsFullAccess

AmazonS3OutpostsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon S3 em Outposts por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonS3OutpostsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de outubro de 2020, 17:26 UTC
- Horário editado: 02 de outubro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*"
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "datasync:ListTasks",
      "datasync:ListLocations",
      "datasync:DescribeTask",
      "datasync:DescribeLocation*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:ListOutposts",
      "outposts:GetOutpost"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonS3OutpostsReadOnlyAccess

AmazonS3OutpostsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon S3 em Outposts por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a AmazonS3OutpostsReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de outubro de 2020, 18:55 UTC
- Horário editado: 02 de outubro de 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
    ],
    "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonS3ReadOnlyAccess

AmazonS3ReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todos os buckets por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a `AmazonS3ReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 10 de agosto de 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função de serviço usada pelo serviço de AWS service (Serviço da AWS) catálogo para provisionar produtos do portfólio de produtos do Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo CodePipeline, CodeBuild, CodeCommit, Glue, CloudFormation etc.

### A utilização desta política

Você pode vincular a AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2020, 18:48 UTC
- Horário editado: 02 de agosto de 2022, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerCanvasAIServiceAccess

AmazonSageMakerCanvasAIServiceAccess é uma [política AWS gerenciada](#) que: Fornece permissões para o Amazon SageMaker Canvas usar serviços de IA para oferecer suporte a soluções de IA prontas para uso. Essa política adicionará mais permissões mutantes para serviços à medida que o Amazon SageMaker Canvas adicionar suporte.

### Utilização desta política

Você pode vincular a AmazonSageMakerCanvasAIServiceAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 23 de março de 2023, 22:36 UTC
- Horário editado: 29 de novembro de 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServiceAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Texttract",
      "Effect" : "Allow",
      "Action" : [
        "texttract:AnalyzeDocument",
        "texttract:AnalyzeExpense",
        "texttract:AnalyzeID",
        "texttract:StartDocumentAnalysis",
        "texttract:StartExpenseAnalysis",
        "texttract:GetDocumentAnalysis",
        "texttract: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"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões para usar o Amazon Bedrock no SageMaker Canvas, fornecendo acesso a serviços downstream, como o S3.

### Utilização desta política

Você pode vincular a AmazonSageMakerCanvasBedrockAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 02 de fevereiro de 2024, 18:37 UTC
- Horário editado: 02 de fevereiro de 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSageMakerCanvasDataPrepFullAccess

AmazonSageMakerCanvasDataPrepFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos SageMaker recursos e operações da Amazon para preparação de dados no Canvas. A política também fornece acesso seletivo a serviços relacionados (por exemplo, S3, IAM, KMS, RDS, Logs, Redshift CloudWatch, Athena, Glue, Secrets Manager). EventBridge Essa política deve ser anexada à função de execução de SageMaker domínio/perfil de usuário da Amazon.

## Utilização desta política

Você pode vincular a AmazonSageMakerCanvasDataPrepFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 27 de outubro de 2023, 22:56 UTC
- Horário editado: 08 de dezembro de 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

```
{
  "Sid" : "SageMakerFeatureGroupOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateFeatureGroup",
    "sagemaker:DescribeFeatureGroup"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
},
{
  "Sid" : "SageMakerProcessingJobOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateProcessingJob",
    "sagemaker:DescribeProcessingJob",
    "sagemaker:AddTags"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
},
{
  "Sid" : "SageMakerProcessingJobListOperation",
  "Effect" : "Allow",
  "Action" : "sagemaker:ListProcessingJobs",
  "Resource" : "*"
},
{
  "Sid" : "SageMakerPipelineOperations",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribePipeline",
    "sagemaker:CreatePipeline",
    "sagemaker:UpdatePipeline",
    "sagemaker>DeletePipeline",
    "sagemaker:StartPipelineExecution",
    "sagemaker:ListPipelineExecutionSteps",
    "sagemaker:DescribePipelineExecution"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
},
{
  "Sid" : "KMSListOperations",
  "Effect" : "Allow",
  "Action" : "kms:ListAliases",
  "Resource" : "*"
}
```

```

},
{
  "Sid" : "KMSOperations",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Sid" : "S3Operations",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:AbortMultipartUpload"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "S3GetObjectOperation",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : "arn:aws:s3::*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/SageMaker" : "true"
    },
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{

```

```
"Sid" : "S3ListOperations",
"Effect" : "Allow",
"Action" : [
  "s3:ListBucket",
  "s3:ListAllMyBuckets"
],
"Resource" : "*"
},
{
  "Sid" : "IAMListOperations",
  "Effect" : "Allow",
  "Action" : "iam:ListRoles",
  "Resource" : "*"
},
{
  "Sid" : "IAMGetOperations",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/*"
},
{
  "Sid" : "IAMPassOperation",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com",
        "events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "EventBridgePutOperation",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events::*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
}
```



```
    }
  }
},
{
  "Sid" : "EventBridgeOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:PutTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeTagBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "events:TagResource"
  ],
  "Resource" : "arn:aws:events:*:*:rule/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
    }
  }
},
{
  "Sid" : "EventBridgeListTagOperation",
  "Effect" : "Allow",
  "Action" : "events:ListTagsForResource",
  "Resource" : "*"
},
{
  "Sid" : "GlueOperations",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
```

```
    "glue:SearchTables"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Sid" : "EMROperations",
  "Effect" : "Allow",
  "Action" : [
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups"
  ],
  "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
},
{
  "Sid" : "EMRListOperation",
  "Effect" : "Allow",
  "Action" : "elasticmapreduce:ListClusters",
  "Resource" : "*"
},
{
  "Sid" : "AthenaListDataCatalogOperation",
  "Effect" : "Allow",
  "Action" : "athena:ListDataCatalogs",
  "Resource" : "*"
},
{
  "Sid" : "AthenaQueryExecutionOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution"
  ],
  "Resource" : "arn:aws:athena:*:*:workgroup/*"
},
{
  "Sid" : "AthenaDataCatalogOperations",
  "Effect" : "Allow",
  "Action" : [
```

```

    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : "arn:aws:athena:*:*:datacatalog/*"
},
{
  "Sid" : "RedshiftOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:DescribeStatement",
    "redshift-data:CancelStatement",
    "redshift-data:GetStatementResult"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RedshiftArnBasedOperations",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ],
  "Resource" : "arn:aws:redshift:*:*:cluster:*"
},
{
  "Sid" : "RedshiftGetCredentialsOperation",
  "Effect" : "Allow",
  "Action" : "redshift:GetClusterCredentials",
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "SecretsManagerARNBasedOperation",
  "Effect" : "Allow",
  "Action" : "secretsmanager:CreateSecret",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
},
{
  "Sid" : "SecretManagerTagBasedOperation",
  "Effect" : "Allow",
  "Action" : [

```

```
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",
  "Action" : "rds:DescribeDBInstances",
  "Resource" : "*"
},
{
  "Sid" : "LoggingOperation",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccess é uma [política AWS gerenciada](#) que: Permite que o Amazon SageMaker Canvas crie, gerencie e visualize detalhes de endpoints para endpoints criados por meio do Canvas. Permite que o Amazon SageMaker Canvas recupere métricas de invocação de endpoints do CloudWatch.

## A utilização desta política

Você pode vincular a AmazonSageMakerCanvasDirectDeployAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de outubro de 2023, 18:11 UTC
- Horário editado: 06 de outubro de 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
```

```
    "sagemaker:CreateEndpointConfig",
    "sagemaker>DeleteEndpoint",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:InvokeEndpoint",
    "sagemaker:UpdateEndpoint"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:Canvas*",
    "arn:aws:sagemaker:*:*:canvas*"
  ]
},
{
  "Sid" : "ReadCWInvocationMetrics",
  "Effect" : "Allow",
  "Action" : "cloudwatch:GetMetricData",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccess é uma [política AWS gerenciada que: Essa política](#) concede as permissões normalmente necessárias para usar o SageMaker Canvas com o Amazon Forecast.

### A utilização desta política

Você pode vincular a AmazonSageMakerCanvasForecastAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de agosto de 2022, 20:04 UTC
- Horário editado: 24 de agosto de 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

```
]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerCanvasFullAccess

AmazonSageMakerCanvasFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos e operações do Amazon SageMaker Canvas. A política também fornece acesso seletivo a serviços relacionados (por exemplo, S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager e Forecast). Essa política deve ser anexada à função de execução de SageMaker domínio/perfil de usuário da Amazon.

### Utilização desta política

Você pode vincular a AmazonSageMakerCanvasFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 09 de setembro de 2022, 00:44 UTC
- Horário editado: 24 de janeiro de 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

### Versão da política

Versão da política: v9 (padrão)



A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",

```

```

    "sagemaker:CreateModel",
    "sagemaker:CreateProcessingJob",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateAutoMLJobV2",
    "sagemaker>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"
      }
    }
  }
]
}

```



## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerClusterInstanceRolePolicy

AmazonSageMakerClusterInstanceRolePolicy é uma [política AWS gerenciada](#) que: Essa política concede as permissões normalmente necessárias para usar o Amazon SageMaker Cluster.

### Utilização desta política

Você pode vincular a AmazonSageMakerClusterInstanceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 29 de novembro de 2023, 15:11 UTC
- Horário editado: 29 de novembro de 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CloudwatchLogStreamPublishPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
    ]
  },
  {
    "Sid" : "CloudwatchLogGroupCreationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
    ]
  },
  {
    "Sid" : "CloudwatchPutMetricDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
      }
    }
  },
  {
    "Sid" : "DataRetrievalFromS3BucketPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",

```

```
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::sagemaker-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "SSMConnectivityPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy é uma [política AWS gerenciada que: Política gerenciada para Service Linked Role para Amazon SageMaker Core Services](#)

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de dezembro de 2020, 21:40 UTC
- Horário editado: 21 de dezembro de 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "ec2:CreateNetworkInterfacePermission"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy é uma [política AWS gerenciada](#) que: Fornece as permissões necessárias para que o SageMaker Edge crie e gereencie uma frota de dispositivos para o cliente usando a conexão de nuvem padrão.

### A utilização desta política

Você pode vincular a AmazonSageMakerEdgeDeviceFleetPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 08 de dezembro de 2020, 16:17 UTC
- Horário editado: 08 de dezembro de 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateIoTRoleAlias",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateRoleAlias",
      "iot:DescribeRoleAlias",
      "iot:UpdateRoleAlias",
      "iot:ListTagsForResource",
      "iot:TagResource"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
    ]
  },
  {
    "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/*SageMaker*",
      "arn:aws:iam:*:*:role/*Sagemaker*",
      "arn:aws:iam:*:*:role/*sagemaker*"
    ]
  },
  {
    "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/*SageMaker*",
      "arn:aws:iam:*:*:role/*Sagemaker*",
      "arn:aws:iam:*:*:role/*sagemaker*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : [
          "iot.amazonaws.com",
```

```
        "credentials.iot.amazonaws.com"  
    ]  
  }  
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerFeatureStoreAccess

AmazonSageMakerFeatureStoreAccess é uma [política AWS gerenciada](#) que: Fornece as permissões necessárias para habilitar a loja off-line para um grupo de recursos do Amazon SageMaker FeatureStore.

### A utilização desta política

Você pode vincular a AmazonSageMakerFeatureStoreAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 16:24 UTC
- Horário editado: 05 de dezembro de 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

### Versão da política

Versão da política: v3 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*/metadata/*",
        "arn:aws:s3::*Sagemaker*/metadata/*",
        "arn:aws:s3::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

```
]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerFullAccess

AmazonSageMakerFullAccess é uma [política AWS gerenciada](#) que: AWS Management Console Fornece acesso total à Amazon SageMaker por meio do SDK. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, ECR, CloudWatch Logs).

### Utilização desta política

Você pode vincular a AmazonSageMakerFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 29 de novembro de 2017, 13:07 UTC
- Horário editado: 30 de novembro de 2023, 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

### Versão da política

Versão da política: v25 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "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" : "*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerGeospatialExecutionRole

AmazonSageMakerGeospatialExecutionRole é uma [política AWS gerenciada](#) que: Essa política fornece acesso aos serviços que normalmente são necessários para usar o SageMaker geoespacial.

## A utilização desta política

Você pode vincular a `AmazonSageMakerGeospatialExecutionRole` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 30 de novembro de 2022, 10:08 UTC
- Horário editado: 10 de maio de 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3::*SageMaker*",
        "arn:aws:s3::*Sagemaker*",
        "arn:aws:s3::*sagemaker*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerGeospatialFullAccess

AmazonSageMakerGeospatialFullAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões que permitem acesso total ao Amazon SageMaker Geospatial por meio do e SDK. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonSageMakerGeospatialFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 30 de novembro de 2022, 10:06 UTC
- Horário editado: 30 de novembro de 2022, 10:06 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS serviços necessários para executar o trabalho de rotulagem do SageMaker GroundTruth

### A utilização desta política

Você pode vincular a AmazonSageMakerGroundTruthExecution aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2020, 19:30 UTC
- Horário editado: 29 de abril de 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:*GtRecipe*",
      "arn:aws:lambda:*:*:function:*LabelingFunction*",
      "arn:aws:lambda:*:*:function:*SageMaker*",
      "arn:aws:lambda:*:*:function:*sagemaker*",
      "arn:aws:lambda:*:*:function:*Sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*GroundTruth*",
      "arn:aws:s3::*Groundtruth*",
      "arn:aws:s3::*groundtruth*",
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/SageMaker" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket"
    ]
  }
}

```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData",
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "StreamingQueue",
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs:DeleteMessage",
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl",
      "sqs:ReceiveMessage",
      "sqs:SendMessage",
      "sqs:SetQueueAttributes"
    ],
    "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
  },
  {
    "Sid" : "StreamingTopicSubscribe",
    "Effect" : "Allow",
    "Action" : "sns:Subscribe",
    "Resource" : [
      "arn:aws:sns:*:*:*GroundTruth*",
      "arn:aws:sns:*:*:*Groundtruth*",
      "arn:aws:sns:*:*:*groundTruth*",
      "arn:aws:sns:*:*:*groundtruth*",
      "arn:aws:sns:*:*:*SageMaker*",
      "arn:aws:sns:*:*:*Sagemaker*",
      "arn:aws:sns:*:*:*sageMaker*",
      "arn:aws:sns:*:*:*sagemaker*"
    ],
    "Condition" : {
```



```
    "StringEquals" : {
      "sns:Protocol" : "sqs"
    },
    "StringLike" : {
      "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
    }
  }
},
{
  "Sid" : "StreamingTopic",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:*GroundTruth*",
    "arn:aws:sns:*:*:*Groundtruth*",
    "arn:aws:sns:*:*:*groundTruth*",
    "arn:aws:sns:*:*:*groundtruth*",
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sageMaker*",
    "arn:aws:sns:*:*:*sagemaker*"
  ]
},
{
  "Sid" : "StreamingTopicUnsubscribe",
  "Effect" : "Allow",
  "Action" : [
    "sns:Unsubscribe"
  ],
  "Resource" : "*"
},
{
  "Sid" : "WorkforceVPC",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
```

```
    "ec2:VpceServiceName" : [
      "*sagemaker-task-resources*",
      "aws.sagemaker*labeling*"
    ]
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerMechanicalTurkAccess

AmazonSageMakerMechanicalTurkAccess é uma [política AWS gerenciada](#) que: Fornece acesso para criar recursos Amazon Augmented AI FlowDefinition contra qualquer equipe de trabalho.

### A utilização desta política

Você pode vincular a AmazonSageMakerMechanicalTurkAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 16:19 UTC
- Horário editado: 03 de dezembro de 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerModelGovernanceUseAccess

AmazonSageMakerModelGovernanceUseAccess é uma [política AWS gerenciada que: Essa política AWS gerenciada concede as permissões necessárias para usar todos os recursos de governança do Amazon SageMaker. A política também fornece acesso seletivo a serviços relacionados \(por exemplo, S3, KMS\).](#)

## A utilização desta política

Você pode vincular a `AmazonSageMakerModelGovernanceUseAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2022, 08:58 UTC
- Horário editado: 17 de julho de 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTrainingJobs",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:ListModels",
    "sagemaker:DescribeModel",
    "sagemaker:Search",
    "sagemaker:AddTags",
    "sagemaker>DeleteTags",
    "sagemaker:ListTags"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:CreateBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ]
},
{
```

```
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccess é uma [política AWS gerenciada](#) que: Essa é uma nova política gerenciada para o Registro de Modelos no Sagemaker. Essa política é uma política independente que pode ser anexada à função do usuário para acessar as funcionalidades relacionadas ao Registro de Modelos no Sagemaker.

### A utilização desta política

Você pode vincular a AmazonSageMakerModelRegistryFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de abril de 2023, 05:20 UTC
- Horário editado: 13 de abril de 2023, 05:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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" : "*"
    },
    {
      "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*SageMaker*",
    "arn:aws:s3:::*Sagemaker*",
    "arn:aws:s3:::*sagemaker*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:DescribeImages"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "sagemaker.amazonaws.com"
    }
  }
},
},
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:GetGroupQuery"
  ],
  "Resource" : "arn:aws:resource-groups:*:*:group/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:ListGroupResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:CreateGroup",
    "resource-groups:Tag"
  ],
  "Resource" : "arn:aws:resource-groups:*:*:group/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "sagemaker:collection"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "resource-groups:DeleteGroup",
  "Resource" : "arn:aws:resource-groups:*:*:group/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:collection" : "true"
    }
  }
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerNotebooksServiceRolePolicy

AmazonSageMakerNotebooksServiceRolePolicy é uma [política AWS gerenciada que: Política gerenciada para Service Linked Role para notebooks Amazon SageMaker](#)

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de outubro de 2019, 20:27 UTC
- Horário editado: 09 de março de 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",

```

```

    "elasticfilesystem:DeleteMountTarget"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticfilesystem:TagResource",
  "Resource" : [
    "arn:aws:elasticfilesystem:*:*:access-point/*",
    "arn:aws:elasticfilesystem:*:*:file-system/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",

```

```

    "ec2:DeleteNetworkInterface",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteManagedApplicationInstance",
    "sso:GetManagedApplicationInstance"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateUserProfile",
    "sagemaker:DescribeUserProfile"
  ],
  "Resource" : "*"
}

```

```
}  
]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função de serviço usada pelo AWS ApiGateway nos produtos AWS provisionados do ServiceCatalog do portfólio de produtos do Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo Lambda e outros.

## A utilização desta política

Você pode vincular a

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de agosto de 2023, 15:06 UTC
- Horário editado: 01 de agosto de 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pelo AWS CloudFormation nos produtos provisionados AWS do ServiceCatalog do portfólio de produtos Amazon SageMaker. Concede permissões a um subconjunto de serviços relacionados, incluindo Lambda, ApiGateway e outros.

### A utilização desta política

Você pode vincular a

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de agosto de 2023, 15:06 UTC
- Horário editado: 01 de agosto de 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
```

```

    "lambda:UpdateFunctionCode",
    "lambda:ListTags",
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda:TagResource"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:sagemaker-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name",
        "sagemaker:partner"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:PublishLayerVersion",
    "lambda:GetLayerVersion",
    "lambda>DeleteLayerVersion",
    "lambda:GetFunction"
  ],

```

```
"Resource" : [
  "arn:aws:lambda:*:*:layer:sagemaker-*",
  "arn:aws:lambda:*:*:function:sagemaker-*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET",
    "apigateway:DELETE",
    "apigateway:PATCH",
    "apigateway:POST",
    "apigateway:PUT"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/restapis/*",
    "arn:aws:apigateway:*:*/restapis"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:POST",
    "apigateway:PUT"
  ],
  "Resource" : [
    "arn:aws:apigateway:*:*/restapis",
    "arn:aws:apigateway:*:*/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/sagemaker:project-name" : "false",
      "aws:ResourceTag/sagemaker:partner" : "false"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name",
        "sagemaker:partner"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pela AWS Lambda nos produtos provisionados do AWS ServiceCatalog do portfólio de produtos Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo Secrets Manager e outros.

## A utilização desta política

Você pode vincular a `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de agosto de 2023, 15:05 UTC
- Horário editado: 01 de agosto de 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerPipelinesIntegrations

AmazonSageMakerPipelinesIntegrations é uma [política AWS gerenciada que: Essa política](#) gerenciada da Amazon concede as permissões normalmente necessárias para uso com etapas de retorno de chamada e etapas Lambda nos pipelines de construção de modelos do SageMaker. Ele é adicionado ao AmazonSageMaker-ExecutionRole que pode ser criado ao configurar o SageMaker Studio. Também pode ser anexado a qualquer outra função que será usada para criar ou executar pipelines.

### A utilização desta política

Você pode vincular a AmazonSageMakerPipelinesIntegrations aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de julho de 2021, 16:35 UTC
- Horário editado: 17 de fevereiro de 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam:*:*:role/*",
      "Condition" : {
```

```
    "StringEquals" : {
      "iam:PassedToService" : [
        "lambda.amazonaws.com",
        "elasticmapreduce.amazonaws.com",
        "ec2.amazonaws.com"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutRule",
      "events:PutTargets"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
      "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:AddJobFlowSteps",
      "elasticmapreduce:CancelSteps",
      "elasticmapreduce:DescribeStep",
      "elasticmapreduce:RunJobFlow",
      "elasticmapreduce:DescribeCluster",
      "elasticmapreduce:TerminateJobFlows",
      "elasticmapreduce:ListSteps"
    ],
    "Resource" : [
      "arn:aws:elasticmapreduce:*:*:cluster/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)



- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerReadOnly

AmazonSageMakerReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon SageMaker por meio AWS Management Console do e SDK.

### A utilização desta política

Você pode vincular a AmazonSageMakerReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 29 de novembro de 2017, 13:07 UTC
- Horário editado: 01 de dezembro de 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

```

    "sagemaker:List*",
    "sagemaker:BatchGetMetrics",
    "sagemaker:GetDeviceRegistration",
    "sagemaker:GetDeviceFleetReport",
    "sagemaker:GetSearchSuggestions",
    "sagemaker:BatchGetRecord",
    "sagemaker:GetRecord",
    "sagemaker:Search",
    "sagemaker:QueryLineage",
    "sagemaker:GetLineageGroupPolicy",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:GetModelPackageGroupPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "aws-marketplace:ViewSubscriptions",
    "cloudwatch:DescribeAlarms",
    "cognito-idp:DescribeUserPool",
    "cognito-idp:DescribeUserPoolClient",
    "cognito-idp:ListGroups",
    "cognito-idp:ListIdentityProviders",
    "cognito-idp:ListUserPoolClients",
    "cognito-idp:ListUserPools",
    "cognito-idp:ListUsers",
    "cognito-idp:ListUsersInGroup",
    "ecr:Describe*"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função de serviço usada pelo AWS ApiGateway nos produtos AWS provisionados do ServiceCatalog do portfólio de produtos do Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo CloudWatch Logs e outros.

### A utilização desta política

Você pode vincular a AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 25 de março de 2022, 04:25 UTC
- Horário editado: 25 de março de 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs>DeleteLogDelivery",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:DescribeResourcePolicies",
      "logs:DescribeDestinations",
      "logs:DescribeExportTasks",
      "logs:DescribeMetricFilters",
      "logs:DescribeQueries",
      "logs:DescribeQueryDefinitions",
      "logs:DescribeSubscriptionFilters",
      "logs:GetLogDelivery",
      "logs:GetLogEvents",
      "logs:PutLogEvents",
      "logs:PutResourcePolicy",
      "logs:UpdateLogDelivery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pelo AWS CloudFormation

nos produtos provisionados AWS do ServiceCatalog do portfólio de produtos Amazon SageMaker. Concede permissões a um subconjunto de serviços relacionados, incluindo o SageMaker e outros.

## A utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 25 de março de 2022, 04:26 UTC
- Horário editado: 25 de março de 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
```

```
"sagemaker:CreateAction",
"sagemaker:CreateAlgorithm",
"sagemaker:CreateApp",
"sagemaker:CreateAppImageConfig",
"sagemaker:CreateArtifact",
"sagemaker:CreateAutoMLJob",
"sagemaker:CreateCodeRepository",
"sagemaker:CreateCompilationJob",
"sagemaker:CreateContext",
"sagemaker:CreateDataQualityJobDefinition",
"sagemaker:CreateDeviceFleet",
"sagemaker:CreateDomain",
"sagemaker:CreateEdgePackagingJob",
"sagemaker:CreateEndpoint",
"sagemaker:CreateEndpointConfig",
"sagemaker:CreateExperiment",
"sagemaker:CreateFeatureGroup",
"sagemaker:CreateFlowDefinition",
"sagemaker:CreateHumanTaskUi",
"sagemaker:CreateHyperParameterTuningJob",
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
```

```
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
"sagemaker>DeleteModelPackageGroup",
"sagemaker>DeleteModelPackageGroupPolicy",
"sagemaker>DeleteModelQualityJobDefinition",
"sagemaker>DeleteMonitoringSchedule",
"sagemaker>DeleteNotebookInstance",
"sagemaker>DeleteNotebookInstanceLifecycleConfig",
"sagemaker>DeletePipeline",
"sagemaker>DeleteProject",
"sagemaker>DeleteRecord",
"sagemaker>DeleteTags",
"sagemaker>DeleteTrial",
"sagemaker>DeleteTrialComponent",
"sagemaker>DeleteUserProfile",
"sagemaker>DeleteWorkforce",
"sagemaker>DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
```

```
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
```



```
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
```

```
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
```

```
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"NotResource" : [
  "arn:aws:sagemaker:*:*:domain/*",
  "arn:aws:sagemaker:*:*:user-profile/*",
  "arn:aws:sagemaker:*:*:app/*",
  "arn:aws:sagemaker:*:*:flow-definition/*"
]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função de serviço usada pelo AWS CodeBuild nos produtos provisionados do ServiceCatalog AWS do portfólio de produtos do Amazon SageMaker. Concede permissões a um subconjunto de serviços relacionados, incluindo CodePipeline, CodeBuild e outros.

## A utilização desta política

Você pode vincular a AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de março de 2022, 04:27 UTC
- Horário editado: 25 de março de 2022, 04:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
```

```

    "ecr:DescribeRepositories",
    "ecr:DescribeImageReplicationStatus",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/sagemaker-*"
  ]
},
{
  "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"
    ]
}
},
{
    "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/*"
},
{
    "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-*"
  ]
},
{
  "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*"
  ]
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função de serviço usada pelo AWS CodePipeline nos produtos provisionados do ServiceCatalog AWS do portfólio de produtos do Amazon SageMaker.

Concede permissões a um subconjunto de serviços relacionados, incluindo CodePipeline, CodeBuild e outros.

## A utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 22 de fevereiro de 2022, 09:53 UTC
- Horário editado: 22 de fevereiro de 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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-*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3::*:sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
    ],
    "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",

```



```
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
    ],
    "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pelo AWS CloudWatch Events no ServiceCatalog provisionou produtos AWS do portfólio de produtos do Amazon SageMaker. Concede permissões a um subconjunto de serviços relacionados, incluindo CodePipeline e outros.

### A utilização desta política

Você pode vincular a AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 22 de fevereiro de 2022, 09:53 UTC
- Horário editado: 22 de fevereiro de 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pelo AWS Firehose nos produtos provisionados do AWS ServiceCatalog do portfólio de produtos do Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo Firehose e outros.

## A utilização desta política

Você pode vincular a `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 22 de fevereiro de 2022, 09:54 UTC
- Horário editado: 22 de fevereiro de 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pelo AWS Glue nos produtos provisionados do AWS ServiceCatalog do portfólio de produtos do Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo Glue, S3 e outros.

### A utilização desta política

Você pode vincular a AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Hora de criação: 22 de fevereiro de 2022, 09:51 UTC
- Horário editado: 26 de agosto de 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue>DeletePartition",
        "glue>DeleteTable",
        "glue>DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery"
  ],

```

```
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy é uma [política AWS gerenciada que: A política](#) de função de serviço usada pela AWS Lambda nos produtos provisionados do AWS ServiceCatalog do portfólio de produtos Amazon SageMaker. Concede permissões a um conjunto de serviços relacionados, incluindo ECR, S3 e outros.

## A utilização desta política

Você pode vincular a AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 04 de abril de 2022, 16:34 UTC
- Horário editado: 04 de abril de 2022, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events>DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/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" : [
    "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:ListModel",
"sagemaker:ListModelingExecutions",
"sagemaker:ListModelingSchedules",
"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/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"

```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSecurityLakeAdministrator

AmazonSecurityLakeAdministrator é uma [política gerenciada pela AWS](#) que: Fornece acesso total ao Amazon Security Lake e aos serviços relacionados necessários para administrar o Security Lake.

## Utilização desta política

Você pode vincular a AmazonSecurityLakeAdministrator aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 30 de maio de 2023, 22:04 UTC
- Horário editado: 23 de fevereiro de 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowManagingSecurityLakeS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ]
  }
}
```

```
    ],
    "Resource" : "arn:aws:s3::aws-security-data-lake*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowLambdaCreateFunction",
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowLambdaAddPermission",
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      },
      "StringEquals" : {
        "lambda:Principal" : "securitylake.amazonaws.com"
      }
    }
  }
},
{
```

```

    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowEventBridgeActions",
    "Effect" : "Allow",
    "Action" : [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
      "events>DeleteConnection",
      "events>DeleteApiDestination",
      "events:ListTargetsByRule",
      "events:RemoveTargets",
      "events>DeleteRule"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/AmazonSecurityLake*",
      "arn:aws:events:*:*:rule/SecurityLake*",
      "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
      "arn:aws:events:*:*:connection/AmazonSecurityLake*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {

```

```
        "aws:CalledVia" : "securitylake.amazonaws.com"
    }
}
},
{
    "Sid" : "AllowSQSActions",
    "Effect" : "Allow",
    "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs>DeleteQueue"
    ],
    "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid" : "AllowKmsCmkGrantForSecurityLake",
    "Effect" : "Allow",
    "Action" : "kms:CreateGrant",
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
            "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
            "kms:GrantOperations" : [
                "GenerateDataKey",
                "RetireGrant",
                "Decrypt"
            ]
        }
    }
}
```

```
    }
  },
  {
    "Sid" : "AllowEnablingQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ram:ResourceArn" : [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowConfiguringQueryBasedSubscribers",
    "Effect" : "Allow",
    "Action" : [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram>DeleteResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : "LakeFormation*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
```

```

    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      },
      "StringLike" : {

```



```

        "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
    },
    "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
    }
}
},
{
    "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
            "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
    }
},
{
    "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
            "iam:AssociatedResourceARN" : "arn:aws:s3::*:aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : "securitylake.amazonaws.com"
        }
    }
}
},
{

```

```

    "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake::*:data-lake/default"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "events.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceARN" : "arn:aws:securitylake::*:subscriber/*"
      }
    }
  }
},

```

```

    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AmazonSecurityLakeMetastoreManager

AmazonSecurityLakeMetastoreManager é uma [política AWS gerenciada que: Política](#) para o gerenciador de SecurityLake meta-armazenamento lambda da Amazon, que permite o acesso ao cloudwatch, S3, Glue e SQS.

## Utilização desta política

Você pode vincular a AmazonSecurityLakeMetastoreManager aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 23 de janeiro de 2024, 15:26 UTC
- Horário editado: 23 de janeiro de 2024, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
      "arn:aws:logs:*:*/aws/lambda/AmazonSecurityLake*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AllowGlueManage",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreatePartition",
      "glue:BatchCreatePartition",
      "glue:GetTable",
      "glue:UpdateTable"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/**",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:catalog"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AllowToReadFromSqs",
    "Effect" : "Allow",
    "Action" : [
      "sqs:ReceiveMessage",
      "sqs>DeleteMessage",
      "sqs:GetQueueAttributes"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition" : {
      "StringEquals" : {

```

```
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
},
{
  "Sid" : "AllowMetaDataReadWrite",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-security-data-lake*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSecurityLakePermissionsBoundary

AmazonSecurityLakePermissionsBoundary é uma [política AWS gerenciada](#) que: O Amazon Security Lake cria funções do IAM para fontes personalizadas de terceiros gravarem dados em um data lake e para que assinantes terceirizados consumam dados de um data lake e usa essa política ao criar essas funções para definir o limite de suas permissões.



## A utilização desta política

Você pode vincular a `AmazonSecurityLakePermissionsBoundary` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2022, 14:11 UTC
- Horário editado: 29 de novembro de 2022, 14:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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" : "*"
},
{
  "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" : "*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation"
  ],
  "NotResource" : [
    "arn:aws:s3:::aws-security-data-lake*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [

```

```

    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com",
        "sqs.*.amazonaws.com"
      ]
    }
  }
},
{
  "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*"
      ]
    }
  }
},
},

```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSESFullAccess

AmazonSESFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon SES por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AmazonSESFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSESReadOnlyAccess

AmazonSESReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso de leitura ao Amazon SES por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a AmazonSESReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSNSFullAccess

AmazonSNSFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon SNS por meio do AWS Management Console

### A utilização desta política

Você pode vincular a AmazonSNSFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "sns:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSNSReadOnlyAccess

AmazonSNSReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon SNS por meio do AWS Management Console

### A utilização desta política

Você pode vincular a AmazonSNSReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSNSRole

AmazonSNSRole é uma [política AWS gerenciada que: Política](#) padrão para a função de serviço do Amazon SNS.

## A utilização desta política

Você pode vincular a AmazonSNSRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSQSFullAccess

AmazonSQSFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon SQS por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonSQSFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSQSReadOnlyAccess

AmazonSQSReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon SQS por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AmazonSQSReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 15 de junho de 2023, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess é uma [política AWS gerenciada](#) do que: fornece acesso para visualizar execuções de automação e enviar decisões de aprovação para a automação aguardando aprovação

### A utilização desta política

Você pode vincular a AmazonSSMAutomationApproverAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de agosto de 2017, 23:07 UTC
- Horário editado: 07 de agosto de 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMAutomationRole

AmazonSSMAutomationRole é uma [política AWS gerenciada](#) que: Fornece permissões para o serviço de automação do EC2 executar atividades definidas nos documentos de automação

### A utilização desta política

Você pode vincular a AmazonSSMAutomationRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de dezembro de 2016, 22:09 UTC
- Horário editado: 24 de julho de 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    }
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateImage",
    "ec2:CopyImage",
    "ec2:DeregisterImage",
    "ec2:DescribeImages",
    "ec2>DeleteSnapshot",
    "ec2:StartInstances",
    "ec2:RunInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:DescribeInstanceStatus",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:DescribeTags",
    "cloudformation:CreateStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
    "cloudformation:UpdateStack",
    "cloudformation>DeleteStack"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:Automation*"
  ]
}
```



```
    ]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMDirectoryServiceAccess

AmazonSSMDirectoryServiceAccess é uma [política AWS gerenciada](#) que: Essa política permite que o SSM Agent acesse o Directory Service em nome do cliente para ingressar no domínio da instância gerenciada.

### A utilização desta política

Você pode vincular a AmazonSSMDirectoryServiceAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de março de 2019, 17:44 UTC
- Horário editado: 15 de março de 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMFullAccess

AmazonSSMFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon SSM.

### A utilização desta política

Você pode vincular a AmazonSSMFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de maio de 2015, 17:39 UTC
- Horário editado: 20 de novembro de 2019, 20:08 UTC

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

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole é uma [política AWS gerenciada](#) que: Função de serviço a ser usada para a janela de manutenção do EC2

### A utilização desta política

Você pode vincular a AmazonSSMMaintenanceWindowRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço

- Horário de criação: 01 de dezembro de 2016, 15:57 UTC
- Horário editado: 27 de julho de 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    }
  ],
  {
```

```
    "Effect" : "Allow",
    "Action" : [
      "states:DescribeExecution",
      "states:StartExecution"
    ],
    "Resource" : [
      "arn:aws:states:*:*:stateMachine:SSM*",
      "arn:aws:states:*:*:execution:SSM*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroup",
      "resource-groups:ListGroupResources"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSSMManagedEC2InstanceDefaultPolicy

AmazonSSMManagedEC2InstanceDefaultPolicy é uma [política AWS gerenciada](#) que: Essa política ativa a funcionalidade do AWS Systems Manager em instâncias do EC2.

## A utilização desta política

Você pode vincular a AmazonSSMManagedEC2InstanceDefaultPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de agosto de 2022, 20:54 UTC
- Horário editado: 30 de agosto de 2022, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AmazonSSMManagedInstanceCore

AmazonSSMManagedInstanceCore é uma [política AWS gerenciada](#) que: A política da função do Amazon EC2 para habilitar a funcionalidade principal do serviço AWS Systems Manager.

## A utilização desta política

Você pode vincular a AmazonSSMManagedInstanceCore aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de março de 2019, 17:22 UTC
- Horário editado: 23 de maio de 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
```

```

    "ssm:ListInstanceAssociations",
    "ssm:PutInventory",
    "ssm:PutComplianceItems",
    "ssm:PutConfigurePackageResult",
    "ssm:UpdateAssociationStatus",
    "ssm:UpdateInstanceAssociationStatus",
    "ssm:UpdateInstanceInformation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2messages:AcknowledgeMessage",
    "ec2messages:DeleteMessage",
    "ec2messages:FailMessage",
    "ec2messages:GetEndpoint",
    "ec2messages:GetMessages",
    "ec2messages:SendReply"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonSSMPatchAssociation

AmazonSSMPatchAssociation é uma [política AWS gerenciada](#) que: Fornece acesso às instâncias secundárias para a operação de associação de patches.

## A utilização desta política

Você pode vincular a AmazonSSMPatchAssociation aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de maio de 2020, 16:00 UTC
- Horário editado: 13 de maio de 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMReadOnlyAccess

AmazonSSMReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao Amazon SSM.

### A utilização desta política

Você pode vincular a AmazonSSMReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de maio de 2015, 17:44 UTC
- Horário editado: 29 de maio de 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS recursos gerenciados ou usados pelo Amazon SSM

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de novembro de 2017, 19:20 UTC
- Horário editado: 14 de setembro de 2022, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ]
    }
  ],
}
```

```
"Resource" : [
  "*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:UpdateServiceSetting",
    "ssm:GetServiceSetting"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
    "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:SSM*",
    "arn:aws:lambda:*:*:function:*:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "states:DescribeExecution",
    "states:StartExecution"
  ],
  "Resource" : [
    "arn:aws:states:*:*:stateMachine:SSM*",
```

```
    "arn:aws:states:*:*:execution:SSM*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "resource-groups: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" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonSumerianFullAccess

AmazonSumerianFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Sumerian.

### A utilização desta política

Você pode vincular a AmazonSumerianFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de abril de 2018, 20:14 UTC
- Horário editado: 24 de abril de 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonTextractFullAccess

AmazonTextractFullAccess é uma [política AWS gerenciada](#) que: Acesso a todas as APIs do Amazon Textract

## A utilização desta política

Você pode vincular a AmazonTextractFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 28 de novembro de 2018, 19:07 UTC
- Horário editado: 28 de novembro de 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonTextractServiceRole

AmazonTextractServiceRole é uma [política AWS gerenciada](#) que: Permite que a Textract ligue para AWS serviços em seu nome.

### A utilização desta política

Você pode vincular a AmazonTextractServiceRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Hora de criação: 28 de novembro de 2018, 19:12 UTC
- Horário editado: 28 de novembro de 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:AmazonTexttract*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonTimestreamConsoleFullAccess

AmazonTimestreamConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total para gerenciar o Amazon Timestream usando o AWS Management Console. Observe que essa política também concede permissões para determinadas operações do KMS e operações para gerenciar suas consultas salvas. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

## A utilização desta política

Você pode vincular a AmazonTimestreamConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2020, 21:47 UTC
- Horário editado: 01 de fevereiro de 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "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" : "*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonTimestreamFullAccess

AmazonTimestreamFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Timestream. Observe que essa política também concede acesso a determinadas operações do KMS. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

### A utilização desta política

Você pode vincular a AmazonTimestreamFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2020, 21:47 UTC
- Horário editado: 26 de novembro de 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "timestream:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "kms:EncryptionContextKeys" : "aws:timestream:database-name"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    },
    "StringLike" : {
      "kms:ViaService" : "timestream.*.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccess é uma [política AWS gerenciada](#) que: fornece acesso administrativo total para criar, atualizar, excluir e listar instâncias do Amazon Timestream InfluxDB e criar e listar grupos de parâmetros. Consulte a documentação para obter as permissões adicionais necessárias.

### Utilização desta política

Você pode vincular a AmazonTimestreamInfluxDBFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 14 de março de 2024, 22:53 UTC
- Horário editado: 14 de março de 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "timestream-influxdb:CreateDbParameterGroup",
      "timestream-influxdb:GetDbParameterGroup",
      "timestream-influxdb:ListDbParameterGroups",
      "timestream-influxdb:CreateDbInstance",
      "timestream-influxdb>DeleteDbInstance",
      "timestream-influxdb:GetDbInstance",
      "timestream-influxdb:ListDbInstances",
      "timestream-influxdb:TagResource",
      "timestream-influxdb:UntagResource",
      "timestream-influxdb:ListTagsForResource",
      "timestream-influxdb:UpdateDbInstance"
    ],
    "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::*:*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonTimestreamInfluxDBServiceRolePolicy

AmazonTimestreamInfluxDBServiceRolePolicy é uma [política AWS gerenciada](#) que: fornece acesso administrativo total para criar, atualizar, excluir e listar instâncias do Amazon Timestream

InfluxDB e criar e listar grupos de parâmetros. Consulte a documentação para obter as permissões adicionais necessárias.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de março de 2024, 18:53 UTC
- Horário editado: 14 de março de 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

```

{
  "Sid" : "CreateEniInSubnetStatement",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Sid" : "CreateEniStatement",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
    }
  }
},
{
  "Sid" : "CreateTagWithEniStatement",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
    },
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateNetworkInterface"
      ]
    }
  }
},
{
  "Sid" : "ManageEniStatement",

```



```

    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
      }
    }
  },
  {
    "Sid" : "PutCloudWatchMetricsStatement",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Timestream/InfluxDB",
          "AWS/Usage"
        ]
      }
    },
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "ManageSecretStatement",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret",
      "secretsmanager>DeleteSecret"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }

```

```
}  
  }  
] }  
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Timestream. A política também fornece permissão para cancelar qualquer consulta em execução. Se estiver usando a CMK gerenciada pelo cliente, consulte a documentação para obter as permissões adicionais necessárias.

### A utilização desta política

Você pode vincular a AmazonTimestreamReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2020, 21:47 UTC
- Horário editado: 28 de fevereiro de 2023, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonTranscribeFullAccess

AmazonTranscribeFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total às operações do Amazon Transcribe

## A utilização desta política

Você pode vincular a AmazonTranscribeFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de abril de 2018, 16:06 UTC
- Horário editado: 04 de abril de 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*transcribe*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonTranscribeReadOnlyAccess

AmazonTranscribeReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso à operação somente de leitura para o Amazon Transcribe

### A utilização desta política

Você pode vincular a AmazonTranscribeReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de abril de 2018, 16:05 UTC
- Horário editado: 04 de abril de 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations é uma [política AWS gerenciada](#) do que: fornece acesso para criar interfaces de rede e as anexar a recursos entre contas

## A utilização desta política

Você pode vincular a AmazonVPCCrossAccountNetworkInterfaceOperations aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de julho de 2017, 20:47 UTC
- Horário editado: 25 de setembro de 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",

```

```

    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignIpv6Addresses",
    "ec2:UnassignIpv6Addresses"
  ],
  "Resource" : [
    "*"
  ]
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonVPCFullAccess

AmazonVPCFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à Amazon VPC por meio do. AWS Management Console

### Utilização desta política

Você pode vincular a AmazonVPCFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 08 de fevereiro de 2024, 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
```

```
"ec2:AssignIpv6Addresses",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2: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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy é uma [política gerenciada pela AWS](#) que: fornece permissões para descrever AWS recursos, executar o Network Access Analyzer e criar ou excluir tags no Network Insights Access Scope e no Network Insights Access Scope Analysis.

### Utilização desta política

Você pode vincular a AmazonVPCNetworkAccessAnalyzerFullAccessPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 15 de junho de 2023, 22:56 UTC
- Hora da edição: 03 de novembro de 2023, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-access-scope/*",
    "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
```



```
    "resource-groups:ListGroupResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonVPCReachabilityAnalyzerFullAccessPolicy

AmazonVPCReachabilityAnalyzerFullAccessPolicy é uma [política gerenciada pela AWS](#) que: fornece permissões para descrever AWS recursos, executar o Reachability Analyzer e criar ou excluir tags no Network Insights Path e no Network Insights Analysis.

## Utilização desta política

Você pode vincular a `AmazonVPCReachabilityAnalyzerFullAccessPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 14 de junho de 2023, 20:12 UTC
- Hora da edição: 03 de novembro de 2023, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ]
},

```

```
"Resource" : [
  "arn*:ec2:*:*:network-insights-path/*",
  "arn*:ec2:*:*:network-insights-analysis/*"
],
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "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" : "*"
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy é

uma [política AWS gerenciada que: Essa política](#) é anexada à função

IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Essa função é implantada nas contas dos membros em uma organização quando a conta de gerenciamento permite acesso confiável ao Reachability Analyzer. Ele fornece permissões para visualizar recursos de toda a organização usando o console do Reachability Analyzer.

## A utilização desta política

Você pode vincular a AmazonVPCReachabilityAnalyzerPathComponentReadPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de maio de 2023, 20:38 UTC
- Horário editado: 01 de maio de 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonVPCReadOnlyAccess

AmazonVPCReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura à Amazon VPC por meio do. AWS Management Console

### Utilização desta política

Você pode vincular a AmazonVPCReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 08 de fevereiro de 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
```

```
    "ec2:DescribeClassicLinkInstances",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeMovingAddresses",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeNetworkInterfacePermissions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeSecurityGroups",
    "ec2: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" : "*"
}
]
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AmazonWorkDocsFullAccess

AmazonWorkDocsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon WorkDocs por meio do AWS Management Console

### A utilização desta política

Você pode vincular a AmazonWorkDocsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de abril de 2020, 23:05 UTC
- Horário editado: 16 de abril de 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "workdocs:*",
      "ds:DescribeDirectories",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon WorkDocs por meio do AWS Management Console

### A utilização desta política

Você pode vincular a AmazonWorkDocsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de janeiro de 2020, 23:49 UTC
- Horário editado: 08 de janeiro de 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkMailEventsServiceRolePolicy

AmazonWorkMailEventsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon WorkMail Events

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de abril de 2019, 16:52 UTC
- Horário editado: 16 de abril de 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkMailFullAccess

AmazonWorkMailFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao WorkMail, Directory Service, SES, EC2 e acesso de leitura aos metadados do KMS.

### A utilização desta política

Você pode vincular a AmazonWorkMailFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 21 de dezembro de 2020, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"ds:AuthorizeApplication",
"ds:CheckAlias",
"ds:CreateAlias",
"ds:CreateDirectory",
"ds:CreateIdentityPoolDirectory",
"ds>DeleteDirectory",
"ds:DescribeDirectories",
"ds:GetDirectoryLimits",
"ds:ListAuthorizedApplications",
"ds:UnauthorizeApplication",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2>DeleteSecurityGroup",
"ec2>DeleteSubnet",
"ec2>DeleteVpc",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeRouteTables",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"route53:ChangeResourceRecordSets",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"route53:GetHostedZone",
"route53domains:CheckDomainAvailability",
"route53domains:ListDomains",
"ses:*",
"workmail:*",
"iam:ListRoles",
"logs:DescribeLogGroups",
"logs:CreateLogGroup",
"logs:PutRetentionPolicy",
"cloudwatch:GetMetricData"
],
"Resource" : "*"

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonWorkMailMessageFlowFullAccess

AmazonWorkMailMessageFlowFullAccess é uma [política AWS gerenciada](#) que: Acesso total às APIs de fluxo de mensagens do WorkMail

## A utilização desta política

Você pode vincular a AmazonWorkMailMessageFlowFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de fevereiro de 2021, 11:08 UTC
- Horário editado: 11 de fevereiro de 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkMailMessageFlowReadOnlyAccess

AmazonWorkMailMessageFlowReadOnlyAccess é uma [política AWS gerenciada](#) que: Acesso somente de leitura às mensagens do WorkMail para a API GetRawMessageContent

### A utilização desta política

Você pode vincular a AmazonWorkMailMessageFlowReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de janeiro de 2021, 12:40 UTC
- Horário editado: 28 de janeiro de 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkMailReadOnlyAccess

AmazonWorkMailReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao WorkMail e ao SES.

### A utilização desta política

Você pode vincular a AmazonWorkMailReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 25 de julho de 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonWorkSpacesAdmin

AmazonWorkSpacesAdmin é uma [política AWS gerenciada](#) que: Fornece acesso às ações administrativas do Amazon WorkSpaces via AWS SDK e CLI.

## A utilização desta política

Você pode vincular a AmazonWorkSpacesAdmin aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de setembro de 2015, 22:21 UTC
- Horário editado: 03 de agosto de 2023, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess é uma [política AWS gerenciada](#) que: Fornece acesso de administrador para empacotar um aplicativo no Amazon WorkSpaces Application Manager.

### A utilização desta política

Você pode vincular a AmazonWorkSpacesApplicationManagerAdminAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de abril de 2015, 14:03 UTC
- Horário editado: 09 de abril de 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonWorkspacesPCAAccess

AmazonWorkspacesPCAAccess é uma [política AWS gerenciada](#) que: Essa política gerenciada fornece acesso administrativo total aos recursos de CA privada do AWS Certificate Manager em seu Conta da AWS para autenticação baseada em certificado.

## A utilização desta política

Você pode vincular a AmazonWorkspacesPCAAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de novembro de 2022, 00:25 UTC
- Horário editado: 08 de novembro de 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
```

```
    "StringLike" : {
      "aws:ResourceTag/euc-private-ca" : "*"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkSpacesSelfServiceAccess

AmazonWorkSpacesSelfServiceAccess é uma [política AWS gerenciada](#) que: Fornece acesso ao serviço de back-end do Amazon WorkSpaces para realizar ações de autoatendimento do Workspace

### A utilização desta política

Você pode vincular a AmazonWorkSpacesSelfServiceAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2019, 19:22 UTC
- Horário editado: 27 de junho de 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkSpacesServiceAccess

AmazonWorkSpacesServiceAccess é uma [política AWS gerenciada](#) que: Fornece acesso à conta do cliente ao serviço AWS WorkSpaces para lançar um Workspace.

## A utilização desta política

Você pode vincular a AmazonWorkSpacesServiceAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2019, 19:19 UTC
- Horário editado: 18 de março de 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon WorkSpaces Web e suas dependências por meio AWS Management Console do SDK e da CLI.

### A utilização desta política

Você pode vincular a AmazonWorkSpacesWebReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2021, 14:20 UTC
- Horário editado: 02 de novembro de 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "workspaces-web:GetIdentityProvider",
    "workspaces-web:GetNetworkSettings",
    "workspaces-web:GetPortal",
    "workspaces-web:GetPortalServiceProviderMetadata",
    "workspaces-web:GetTrustStore",
    "workspaces-web:GetTrustStoreCertificate",
    "workspaces-web:GetUserSettings",
    "workspaces-web:GetUserAccessLoggingSettings",
    "workspaces-web:ListBrowserSettings",
    "workspaces-web:ListIdentityProviders",
    "workspaces-web:ListNetworkSettings",
    "workspaces-web:ListPortals",
    "workspaces-web:ListTagsForResource",
    "workspaces-web:ListTrustStoreCertificates",
    "workspaces-web:ListTrustStores",
    "workspaces-web:ListUserSettings",
    "workspaces-web:ListUserAccessLoggingSettings"
  ],
  "Resource" : "arn:aws:workspaces-web:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "kinesis:ListStreams"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon WorkSpaces Web

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de novembro de 2021, 13:15 UTC
- Horário editado: 15 de dezembro de 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
```

```
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/WorkSpacesWebManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "WorkSpacesWebManaged"
      ]
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/WorkSpacesWebManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/WorkSpacesWeb",
          "AWS/Usage"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:PutRecord",
      "kinesis:PutRecords",
      "kinesis:DescribeStreamSummary"
    ],
    "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
  }
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonZocaloFullAccess

AmazonZocaloFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Zocalo.

### A utilização desta política

Você pode vincular a AmazonZocaloFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Action" : [
  "zocalo:*",
  "ds:*",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:CreateNetworkInterface",
  "ec2:CreateSecurityGroup",
  "ec2:CreateSubnet",
  "ec2:CreateTags",
  "ec2:CreateVpc",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcs",
  "ec2>DeleteNetworkInterface",
  "ec2>DeleteSecurityGroup",
  "ec2:RevokeSecurityGroupEgress",
  "ec2:RevokeSecurityGroupIngress"
],
"Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmazonZocaloReadOnlyAccess

AmazonZocaloReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Zocalo

### A utilização desta política

Você pode vincular a AmazonZocaloReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccess é uma [política AWS gerenciada](#) que: Fornece permissões de acesso total ao Amplify para implantar recursos de back-end do Amplify (Amazon AWS AppSync Cognito, Amazon S3 e outros serviços relacionados) por meio do Kit de Desenvolvimento (CDK) Nuvem AWS AWS

### Utilização desta política

Você pode vincular a AmplifyBackendDeployFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 06 de outubro de 2023, 21:32 UTC
- Horário editado: 02 de janeiro de 2024, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

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

```
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:GetTemplate",
    "cloudformation:ListStackResources",
    "cloudformation:GetTemplateSummary"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/amplify-*",
    "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
  ]
},
{
  "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" : "AmplifyHotSwappableSchemaResource",
  "Effect" : "Allow",
  "Action" : [
```

```

    "lambda:InvokeFunction",
    "lambda:UpdateFunctionCode"
  ],
  "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/*"
    ],
    "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}"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o API Gateway gerencie AWS os recursos associados em nome do cliente.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de outubro de 2017, 17:23 UTC
- Horário editado: 12 de julho de 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "elasticloadbalancing:RemoveListenerCertificates",
    "elasticloadbalancing:ModifyListener",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancers",
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingTargets",
    "xray:GetSamplingRules",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:ListLogDeliveries",
    "servicediscovery:DiscoverInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "firehose:DescribeDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch"
  ],
  "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate",
    "acm:GetCertificate"
  ],
  "Resource" : "arn:aws:acm:*:*:certificate/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterfacePermission",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",

```



```

    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Owner",
          "VpcLinkId"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2>DeleteNetworkInterface",
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeNetworkInterfacePermissions",
      "ec2:UnassignPrivateIpAddresses",
      "ec2:DescribeSubnets",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "servicediscovery:GetNamespace",
    "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
  },
  {
    "Effect" : "Allow",
    "Action" : "servicediscovery:GetService",
    "Resource" : "arn:aws:servicediscovery:*:*:service/*"
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: permite que a AppIntegrations gerencie recursos do AppFlow e publique dados métricos do CloudWatch em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de setembro de 2022, 19:42 UTC
- Horário editado: 30 de setembro de 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/AppIntegrations"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:DescribeConnectorEntity",
      "appflow:ListConnectorEntities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:DescribeConnectorProfiles",
      "appflow:UseConnectorProfile"
    ],
    "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow>DeleteFlow",
      "appflow:DescribeFlow",
      "appflow:DescribeFlowExecutionRecords",
      "appflow:StartFlow",
      "appflow:StopFlow",
      "appflow:UpdateFlow"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AppIntegrationsManaged" : "true"
      }
    }
  },
],
```

```
    "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "appflow:TagResource"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AppIntegrationsManaged"
        ]
      }
    },
    "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ApplicationAutoScalingForAmazonAppStreamAccess

ApplicationAutoScalingForAmazonAppStreamAccess é uma [política AWS gerenciada que: Política](#) para habilitar o escalonamento automático de aplicativos para o Amazon AppStream

### A utilização desta política

Você pode vincular a ApplicationAutoScalingForAmazonAppStreamAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2017, 21:39 UTC
- Horário editado: 06 de fevereiro de 2017, 21:39 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo recurso de exportação contínua do Application Discovery Service

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de agosto de 2018, 20:22 UTC
- Horário editado: 13 de agosto de 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "glue:CreateDatabase",
    "glue:UpdateDatabase",
    "glue:CreateTable",
    "glue:UpdateTable",
    "firehose:CreateDeliveryStream",
    "firehose:DescribeDeliveryStream",
    "logs:CreateLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "firehose>DeleteDeliveryStream",
    "firehose:PutRecord",
    "firehose:PutRecordBatch",
    "firehose:UpdateDestination"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
},
{
  "Action" : [
    "s3:CreateBucket",
    "s3:ListBucket",
    "s3:PutBucketLogging",
    "s3:PutEncryptionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
},
{
  "Action" : [
    "s3:GetObject"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
},
{
  "Action" : [
    "logs:CreateLogStream",
```

```
    "logs:PutRetentionPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "firehose.amazonaws.com"
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "firehose.amazonaws.com"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS AppRunner Networking gerencie AWS recursos relacionados em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de janeiro de 2022, 21:02 UTC
- Horário editado: 12 de janeiro de 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkInterface",
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "AWSAppRunnerManaged"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "StringLike" : {
        "aws:RequestTag/AWSAppRunnerManaged" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2>DeleteNetworkInterface",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
      }
    }
  }
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS AppRunner gerencie AWS recursos relacionados em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de maio de 2021, 19:15 UTC
- Horário editado: 14 de maio de 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:RemoveTargets",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AutoScalingConsoleFullAccess

AutoScalingConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Auto Scaling por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a AutoScalingConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2017, 19:43 UTC
- Horário editado: 06 de fevereiro de 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
```

```
    "ec2:DescribeKeyPairs",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcClassicLink",
    "ec2:ImportKeyPair"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:Describe*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:ListMetrics",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:Describe*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "autoscaling:*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:ListSubscriptions",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:ListRoles",
  "Resource" : "*"
}
```

```
    },  
    {  
      "Effect" : "Allow",  
      "Action" : "iam:CreateServiceLinkedRole",  
      "Resource" : "*",  
      "Condition" : {  
        "StringEquals" : {  
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"  
        }  
      }  
    }  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AutoScalingConsoleReadOnlyAccess

AutoScalingConsoleReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Auto Scaling por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AutoScalingConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2017, 19:48 UTC
- Horário editado: 12 de janeiro de 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```



```
    "Effect" : "Allow",
    "Action" : [
      "sns:ListSubscriptions",
      "sns:ListTopics"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AutoScalingFullAccess

AutoScalingFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Auto Scaling.

### A utilização desta política

Você pode vincular a AutoScalingFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2017, 19:31 UTC
- Horário editado: 06 de fevereiro de 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
    },
  ]
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "autoscaling.amazonaws.com"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AutoScalingNotificationAccessRole

AutoScalingNotificationAccessRole é uma [política AWS gerenciada que: Política](#) padrão para a função de serviço AutoScaling Notification Access.

### A utilização desta política

Você pode vincular a AutoScalingNotificationAccessRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AutoScalingReadOnlyAccess

AutoScalingReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao ajuste de escala automático.

## A utilização desta política

Você pode vincular a AutoScalingReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2017, 19:39 UTC
- Horário editado: 12 de janeiro de 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AutoScalingServiceRolePolicy

AutoScalingServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Auto Scaling

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de janeiro de 2018, 23:10 UTC
- Horário editado: 29 de fevereiro de 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    }
  ],
  {
    "Sid" : "EC2SpotManagement",
    "Effect" : "Allow",
```

```
"Action" : [
  "iam:CreateServiceLinkedRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:AWSServiceName" : "spot.amazonaws.com"
  }
}
},
{
  "Sid" : "ELBManagement",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:Register*",
    "elasticloadbalancing:Deregister*",
    "elasticloadbalancing:Describe*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWManagement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSManagement",
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EventBridgeRuleManagement",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
```



```
    "events:PutTargets",
    "events:RemoveTargets",
    "events>DeleteRule",
    "events:DescribeRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "SystemsManagerParameterManagement",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VpcLatticeManagement",
  "Effect" : "Allow",
  "Action" : [
    "vpc-lattice:DeregisterTargets",
    "vpc-lattice:GetTargetGroup",
    "vpc-lattice:ListTargets",
    "vpc-lattice:ListTargetGroups",
    "vpc-lattice:RegisterTargets"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AWS\_ConfigRole

AWS\_ConfigRole é uma [política AWS gerenciada](#) que: Política padrão para a função de serviço AWS Config. Fornece as permissões necessárias para que o AWS Config acompanhe as alterações em seus AWS recursos.

## Utilização desta política

Você pode vincular a AWS\_ConfigRole aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 15 de setembro de 2020, 20:30 UTC
- Horário editado: 22 de fevereiro de 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

## Versão da política

Versão da política: v30 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",

```

```
"acm-pca:DescribeCertificateAuthority",
"acm-pca:GetCertificateAuthorityCertificate",
"acm-pca:GetCertificateAuthorityCsr",
"acm-pca:ListCertificateAuthorities",
"acm-pca:ListTags",
"acm:DescribeCertificate",
"acm:ListCertificates",
"acm:ListTagsForCertificate",
"airflow:GetEnvironment",
"airflow:ListEnvironments",
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:ListApps",
"amplify:ListBranches",
"amplifyuibuilder:ExportThemes",
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"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",
"apppmesh: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" : "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/*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSAccountActivityAccess

AWSAccountActivityAccess é uma [política AWS gerenciada](#) que: Permite que os usuários acessem a página Atividade da conta.

### A utilização desta política

Você pode vincular a AWSAccountActivityAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 07 de março de 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAccountManagementFullAccess

AWSAccountManagementFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao gerenciamento de AWS contas.

### A utilização desta política

Você pode vincular a AWSAccountManagementFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2021, 23:20 UTC
- Horário editado: 30 de setembro de 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para AWS leitura ao gerenciamento de contas

### A utilização desta política

Você pode vincular a AWSAccountManagementReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2021, 23:29 UTC
- Horário editado: 30 de setembro de 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAccountUsageReportAccess

AWSAccountUsageReportAccess é uma [política AWS gerenciada](#) que: Permite que os usuários acessem a página do Relatório de Uso da Conta.

### A utilização desta política

Você pode vincular a AWSAccountUsageReportAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAgentlessDiscoveryService

AWSAgentlessDiscoveryService é uma [política AWS gerenciada](#) que: Fornece acesso ao Discovery Agentless Connector para se registrar no AWS Application Discovery Service.

## A utilização desta política

Você pode vincular a `AWSAgentlessDiscoveryService` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de agosto de 2016, 01:35 UTC
- Horário editado: 24 de fevereiro de 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```

    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::connector-platform-upgrade-info/*",
    "arn:aws:s3:::connector-platform-upgrade-info",
    "arn:aws:s3:::connector-platform-upgrade-bundles/*",
    "arn:aws:s3:::connector-platform-upgrade-bundles",
    "arn:aws:s3:::connector-platform-release-notes/*",
    "arn:aws:s3:::connector-platform-release-notes",
    "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
    "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
},
{
  "Sid" : "Discovery",
  "Effect" : "Allow",
  "Action" : [
    "Discovery:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "arsenal",
  "Effect" : "Allow",
  "Action" : [
    "arsenal:RegisterOnPremisesAgent"
  ]
}

```



```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppFabricFullAccess

AWSAppFabricFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao serviço AWS AppFabric e acesso somente de leitura a serviços dependentes, como S3, Kinesis, KMS.

### A utilização desta política

Você pode vincular a AWSAppFabricFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2023, 19:51 UTC
- Horário editado: 27 de junho de 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowUseOfServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "appfabric.amazonaws.com"
      }
    },
    "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppFabricReadOnlyAccess

AWSAppFabricReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS AppFabric

### A utilização desta política

Você pode vincular a AWSAppFabricReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 27 de junho de 2023, 19:52 UTC
- Horário editado: 27 de junho de 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece ao AppFabric acesso aos AWS recursos em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de junho de 2023, 21:07 UTC
- Horário editado: 26 de junho de 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/AppFabric"
      }
    }
  },
  {
    "Sid" : "S3PutObject",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
    "Condition" : {
      "StringEquals" : {
        "s3:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "FirehosePutRecord",
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecordBatch"
    ],
    "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "aws:ResourceTag/AWSAppFabricManaged" : "true"
      }
    }
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy é uma [política AWS gerenciada](#) que concede permissões ao Application Auto Scaling para acessar o AppStream e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de outubro de 2017, 19:04 UTC
- Horário editado: 20 de outubro de 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "appstream:UpdateFleet",
      "appstream:DescribeFleets",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy é uma [política AWS gerenciada](#) [que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Cassandra e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de março de 2020, 22:49 UTC
- Horário editado: 18 de março de 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSApplicationAutoscalingComprehendEndpointPolicy

AWSApplicationAutoscalingComprehendEndpointPolicy é uma [política AWS gerenciada](#) que concede permissões ao Application Auto Scaling para acessar o Comprehend e o CloudWatch.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de novembro de 2019, 18:39 UTC
- Horário editado: 14 de novembro de 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o ApiGateway e o CloudWatch para escalabilidade personalizada de recursos

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de junho de 2018, 23:22 UTC
- Horário editado: 04 de junho de 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o DynamoDB e o CloudWatch.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de outubro de 2017, 21:34 UTC
- Horário editado: 20 de outubro de 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy é uma [política AWS gerenciada](#) que concede permissões ao Application Auto Scaling para acessar o EC2 Spot Fleet e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 25 de outubro de 2017, 18:23 UTC
- Horário editado: 25 de outubro de 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "ec2:DescribeSpotFleetRequests",
      "ec2:ModifySpotFleetRequest",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o EC2 Container Service e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 25 de outubro de 2017, 23:53 UTC
- Horário editado: 25 de outubro de 2017, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Amazon ElastiCache e o Amazon CloudWatch.



## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de agosto de 2021, 23:41 UTC
- Horário editado: 17 de agosto de 2021, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingEMRInstanceGroupPolicy

AWSApplicationAutoscalingEMRInstanceGroupPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Elastic Map Reduce e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de outubro de 2017, 00:57 UTC
- Horário editado: 26 de outubro de 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Managed Streaming para Apache Kafka e CloudWatch.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de agosto de 2020, 18:36 UTC
- Horário editado: 24 de agosto de 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
  ]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy é uma [política AWS gerenciada](#) [que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Lambda e o CloudWatch.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de outubro de 2019, 20:04 UTC
- Horário editado: 21 de outubro de 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o Amazon Neptune e o Amazon CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de setembro de 2021, 21:14 UTC
- Horário editado: 02 de setembro de 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "rds:DatabaseEngine" : "neptune"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "rds:CreateDBInstance",
    "Resource" : [
      "arn:aws:rds:*:*:db:autoscaled-reader*",
      "arn:aws:rds:*:*:cluster:*"
    ],
    "Condition" : {
      "StringEquals" : {
        "rds:DatabaseEngine" : "neptune"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "rds>DeleteDBInstance"
    ],
    "Resource" : [
      "arn:aws:rds:*:*:db:autoscaled-reader*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
    ]
  }
]
```



## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao Application Auto Scaling para acessar o RDS e o CloudWatch.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de outubro de 2017, 17:46 UTC
- Horário editado: 07 de agosto de 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:CreateDBInstance",
    "rds>DeleteDBInstance",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "rds:ModifyDBCluster",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DescribeAlarms",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "rds.amazonaws.com"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationAutoscalingSageMakerEndpointPolicy

AWSApplicationAutoscalingSageMakerEndpointPolicy é uma [política AWS gerenciada](#) que concede permissões ao Application Auto Scaling para acessar e. SageMaker CloudWatch

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 06 de fevereiro de 2018, 19:58 UTC
- Hora da edição: 13 de novembro de 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ]
    }
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "SageMakerCloudWatchUpdate",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DeleteAlarms"
    ],
    "Resource" : [
      "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
    ]
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess é uma [política AWS gerenciada](#) que: Fornece acesso ao Discovery Agent para se registrar no AWS Application Discovery Service.

### A utilização desta política

Você pode vincular a AWSApplicationDiscoveryAgentAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2016, 21:38 UTC
- Horário editado: 24 de fevereiro de 2020, 22:26 UTC

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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess é uma [política AWS gerenciada](#) que: Permite que os coletores sem agente do Application Discovery Service atualizem, registrem e se comuniquem automaticamente com o Application Discovery Service

## A utilização desta política

Você pode vincular a AWSApplicationDiscoveryAgentlessCollectorAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de agosto de 2022, 21:00 UTC
- Horário editado: 16 de agosto de 2022, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr-public:DescribeImages"
    ],
    "Resource" : "arn:aws:ecr-
public::44637222237: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" : "*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total para visualizar e marcar itens de configuração mantidos pelo AWS Application Discovery Service

## A utilização desta política

Você pode vincular a AWSApplicationDiscoveryServiceFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2016, 21:30 UTC
- Horário editado: 19 de junho de 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



```
{
  "Action" : [
    "iam:GetRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam>DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "migrationhub.amazonaws.com",
        "dmsintegration.migrationhub.amazonaws.com",
        "smsintegration.migrationhub.amazonaws.com"
      ]
    }
  }
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationAgentInstallationPolicy

AWSApplicationMigrationAgentInstallationPolicy é uma [política AWS gerenciada](#) que: Essa política permite instalar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o AWS. Anexe essa política aos usuários ou funções do IAM cujas credenciais você fornece ao instalar o Agente de AWS Replicação.

## A utilização desta política

Você pode vincular a AWSApplicationMigrationAgentInstallationPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de junho de 2022, 07:51 UTC
- Horário editado: 20 de setembro de 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationAgentPolicy

AWSApplicationMigrationAgentPolicy é uma [política AWS gerenciada](#) que: Essa política permite instalar e usar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o AWS. Anexe essa política aos usuários ou funções do IAM cujas credenciais você fornece ao instalar o Agente de AWS Replicação.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationAgentPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de abril de 2021, 07:00 UTC
- Horário editado: 20 de setembro de 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationAgentPolicy\_v2

AWSApplicationMigrationAgentPolicy\_v2 é uma [política AWS gerenciada](#) que: Essa política permite usar o Agente de AWS Replicação, que é usado com o Serviço de Migração de AWS Aplicativos (MGN) para migrar servidores externos para o. AWS Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationAgentPolicy\_v2 aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de junho de 2022, 14:14 UTC
- Horário editado: 06 de junho de 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "mgn:SendAgentMetricsForMgn",
      "mgn:SendAgentLogsForMgn",
      "mgn:UpdateAgentSourcePropertiesForMgn",
      "mgn:UpdateAgentReplicationInfoForMgn",
      "mgn:UpdateAgentConversionInfoForMgn",
      "mgn:GetAgentCommandForMgn",
      "mgn:GetAgentConfirmedResumeInfoForMgn",
      "mgn:GetAgentRuntimeConfigurationForMgn",
      "mgn:UpdateAgentBacklogForMgn",
      "mgn:GetAgentReplicationInfoForMgn",
      "mgn:IssueClientCertificateForMgn"
    ],
    "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationConversionServerPolicy

AWSApplicationMigrationConversionServerPolicy é uma [política AWS gerenciada que: Essa política](#) permite que o Servidor de Conversão do Serviço de Migração de Aplicativos (MGN), que são instâncias do EC2 lançadas pelo Serviço de Migração de Aplicativos, se comunique com o serviço MGN. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela MGN aos servidores de conversão da MGN, que são iniciados e encerrados automaticamente pela MGN, quando necessário. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM. Os servidores de conversão MGN são usados pelo Application Migration Service

quando os usuários optam por iniciar instâncias de teste ou transferência usando o console, a CLI ou a API do MGN.

## A utilização desta política

Você pode vincular a `AWSApplicationMigrationConversionServerPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de abril de 2021, 06:48 UTC
- Horário editado: 07 de abril de 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access é uma [política AWS gerenciada](#) que: Essa política fornece ao Amazon EC2 as operações necessárias para usar o Application Migration Service (MGN) para iniciar os servidores migrados como instâncias do EC2. Anexe essa política aos seus usuários ou funções do IAM.

## A utilização desta política

Você pode vincular a AWSApplicationMigrationEC2Access aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de abril de 2021, 07:05 UTC
- Horário editado: 06 de fevereiro de 2023, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
        "mgn.amazonaws.com"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "mgn.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
```

```
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "mgn.amazonaws.com"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
```

```
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
```

```
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "Null" : {
    "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
```

```
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:launch-template*"
  ],
  "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"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSApplicationMigrationFullAccess

AWSApplicationMigrationFullAccess é uma [política AWS gerenciada](#) que: Essa política fornece permissões para todas as APIs públicas do Serviço de Migração de AWS Aplicativos (MGN), bem como permissões para ler as principais informações do KMS. Anexe essa política aos seus usuários ou funções do IAM.

## A utilização desta política

Você pode vincular a AWSApplicationMigrationFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de abril de 2021, 06:56 UTC
- Horário editado: 20 de abril de 2023, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
},
{
  "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
},
}
```

```

{
  "Effect" : "Allow",
  "Action" : "iam:ListInstanceProfiles",
  "Resource" : "*"
},
{
  "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"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "drs:DescribeSourceServers"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    },
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListCommandInvocations"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
    "arn:aws:ssm:*:*:document/AWSMigration-*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "drs:DisconnectSourceServer"
  ],
}
```

```

    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "Bool" : {
        "aws:ViaAWSService" : "true"
      },
      "Null" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter",
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
      "arn:aws:ssm:*:*:document/AWSMigration-*"
    ]
  },
  {

```

```

    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
**",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "mgn.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ssm:ListCommands",
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationMGHAccess

AWSApplicationMigrationMGHAccess é uma [política AWS gerenciada que: Essa política](#) permite que o Serviço de Migração de AWS Aplicativos (MGN) envie metadados sobre o progresso dos servidores que estão sendo migrados usando o MGN para o Migration AWS Hub (MGH). A MGN cria automaticamente uma função do IAM com essa política anexada e assume essa função. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationMGHAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de abril de 2021, 07:10 UTC
- Horário editado: 07 de abril de 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Effect" : "Allow",
"Action" : [
  "mgh:AssociateCreatedArtifact",
  "mgh:CreateProgressUpdateStream",
  "mgh:DisassociateCreatedArtifact",
  "mgh:GetHomeRegion",
  "mgh:ImportMigrationTask",
  "mgh:NotifyMigrationTaskState",
  "mgh:PutResourceAttributes"
],
"Resource" : "*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationReadOnlyAccess

AWSApplicationMigrationReadOnlyAccess é uma [política AWS gerenciada](#) que: Essa política fornece permissões para todas as APIs públicas somente para leitura do Serviço de Migração de Aplicativos (MGN), bem como algumas APIs somente para leitura de outros AWS serviços que são necessárias para fazer uso total do console do MGN em somente leitura. Anexe essa política aos seus usuários ou funções do IAM.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 07 de abril de 2021, 07:15 UTC
- Horário editado: 20 de março de 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationReplicationServerPolicy

AWSApplicationMigrationReplicationServerPolicy é uma [política AWS gerenciada que: Essa política](#) permite que os servidores de replicação do Serviço de Migração de Aplicativos (MGN), que são instâncias EC2 lançadas pelo Serviço de Migração de Aplicativos, se comuniquem com o serviço MGN e criem instantâneos do EBS em seu. Conta da AWS Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pelo Application Migration Service aos servidores de replicação da MGN, que são automaticamente iniciados e encerrados pela MGN, conforme necessário. Os servidores de replicação MGN são usados para facilitar a replicação de dados de seus servidores externos para AWS, como parte do processo de migração gerenciado usando o MGN. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

## A utilização desta política

Você pode vincular a `AWSApplicationMigrationReplicationServerPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de abril de 2021, 07:21 UTC
- Horário editado: 07 de abril de 2021, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",

```

```
    "mgn:NotifyAgentReplicationProgressForMgn",
    "mgn:NotifyAgentConnectedForMgn",
    "mgn:NotifyAgentDisconnectedForMgn"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
```

```
        "ec2:CreateAction" : "CreateSnapshot"
    }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy é uma [política gerenciada pela AWS](#) que: Essa política permite instalar e usar o Agente de Replicação da AWS, que é usado pelo Serviço de Migração de Aplicativos da AWS (AWS MGN) para migrar servidores de origem executados no EC2 (entre regiões ou entre AZ). Uma função do IAM com essa política deve ser anexada (como um perfil de instância do EC2) às instâncias do EC2.

### Utilização desta política

Você pode vincular a AWSApplicationMigrationServiceEc2InstancePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 22 de agosto de 2023, 13:19 UTC
- Horário editado: 03 de janeiro de 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
```

```
    "Action" : "mgn:TagResource",
    "Resource" : "arn:aws:mgn:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "mgn:CreateAction" : "RegisterAgentForMgn"
      }
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Serviço de Migração de AWS Aplicativos crie e gerencie AWS recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de abril de 2021, 06:43 UTC
- Horário editado: 20 de junho de 2023, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
```

```

    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount"
  ],
  "Resource" : "arn:aws:organizations::*:account/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteSnapshot"
  ],

```

```
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
}
```

```
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
      }
    }
  }
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
},
```

```

{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
    "arn:aws:iam:*:*:role/service-role/AWSApplicationMigrationConversionServerRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate",
        "CreateSecurityGroup",
        "CreateVolume",

```

```
        "CreateSnapshot",
        "RunInstances"
    ]
}
}
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess é uma [política AWS gerenciada](#) que: Essa política fornece acesso às operações do Amazon SSM necessárias para usar o Application Migration Service (MGN) para executar documentos SSM personalizados de comando de pós-migração. Anexe essa política aos seus usuários ou funções do IAM.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationSSMAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 09:29 UTC
- Horário editado: 20 de março de 2023, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

### Versão da política

Versão da política: v2 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-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/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicy é uma [política AWS gerenciada](#) que: Essa política permite instalar e usar o AWS vCenter Client, que é usado com o AWS Application Migration Service (MGN) para migrar servidores externos para o. AWS Anexe essa política aos usuários ou funções do IAM cujas credenciais você fornece ao instalar o AWS vCenter Client.

### A utilização desta política

Você pode vincular a AWSApplicationMigrationVCenterClientPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de novembro de 2021, 12:53 UTC
- Horário editado: 08 de novembro de 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "mgn:CreateVcenterClientForMgn",
    "mgn:DescribeVcenterClients"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "mgn:GetVcenterClientCommandsForMgn",
    "mgn:SendVcenterClientCommandResultForMgn",
    "mgn:SendVcenterClientLogsForMgn",
    "mgn:SendVcenterClientMetricsForMgn",
    "mgn>DeleteVcenterClient",
    "mgn:TagResource",
    "mgn:NotifyVcenterClientStartedForMgn"
  ],
  "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess é uma [política AWS gerenciada que: política](#) do App Mesh Envoy para acessar a configuração do Virtual Node.

### A utilização desta política

Você pode vincular a AWSAppMeshEnvoyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de julho de 2019, 21:29 UTC
- Horário editado: 03 de julho de 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSAppMeshFullAccess

AWSAppMeshFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total às APIs do AWS App Mesh e ao Management Console.

## A utilização desta política

Você pode vincular a AWSAppMeshFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de abril de 2019, 17:50 UTC
- Horário editado: 07 de janeiro de 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "appmesh.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStack*",
      "cloudformation:UpdateStack"
    ],
    "Resource" : "arn:aws:cloudformation::*:stack/AWSAppMesh-GettingStarted-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:ListNamespaces",
      "servicediscovery:ListServices",
      "servicediscovery:ListInstances"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess é uma [política AWS gerenciada que: política](#) do App Mesh Preview Envoy para acessar a configuração do Virtual Node.

### A utilização desta política

Você pode vincular a AWSAppMeshPreviewEnvoyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de agosto de 2019, 23:32 UTC
- Horário editado: 05 de agosto de 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppMeshPreviewServiceRolePolicy

AWSAppMeshPreviewServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS App Mesh

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de junho de 2019, 19:07 UTC
- Horário editado: 21 de agosto de 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSAppMeshReadOnly

AWSAppMeshReadOnly é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura às APIs do AWS App Mesh e ao Management Console.

## A utilização desta política

Você pode vincular a AWSAppMeshReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de abril de 2019, 17:51 UTC
- Horário editado: 07 de janeiro de 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:DescribeStack*"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm:ListCertificates",
      "acm:DescribeCertificate",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicediscovery:ListNamespaces",
      "servicediscovery:ListServices",
      "servicediscovery:ListInstances"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS AppMesh

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de junho de 2019, 18:30 UTC
- Horário editado: 10 de outubro de 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
    }
  ]
}
```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppRunnerFullAccess

`AWSAppRunnerFullAccess` é uma [política AWS gerenciada](#) que: concede permissões para todas as ações do App Runner.

### A utilização desta política

Você pode vincular a `AWSAppRunnerFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de janeiro de 2022, 04:02 UTC
- Horário editado: 11 de janeiro de 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "apprunner.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "apprunner.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AppRunnerAdminAccess",
    "Effect" : "Allow",
    "Action" : "apprunner:*",
    "Resource" : "*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSAppRunnerReadOnlyAccess

`AWSAppRunnerReadOnlyAccess` é uma [política AWS gerenciada](#) que: concede permissões para listar e visualizar detalhes sobre os recursos do App Runner.

## A utilização desta política

Você pode vincular a `AWSAppRunnerReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de fevereiro de 2022, 21:24 UTC
- Horário editado: 24 de fevereiro de 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppRunnerServicePolicyForECRAccess

`AWSAppRunnerServicePolicyForECRAccess` é uma [política AWS gerenciada](#) que: política de serviço AWS App Runner que concede permissões de leitura aos recursos do Amazon ECR na conta do cliente. Use-o em uma função que é passada para o App Runner ao criar ou atualizar um serviço do App Runner.

### A utilização desta política

Você pode vincular a `AWSAppRunnerServicePolicyForECRAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de maio de 2021, 19:17 UTC
- Horário editado: 14 de maio de 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppSyncAdministrator

AWSAppSyncAdministrator é uma [política AWS gerenciada](#) que: fornece acesso administrativo ao serviço AppSync, mas não o suficiente para acesso pelo console.

### A utilização desta política

Você pode vincular a AWSAppSyncAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 20 de março de 2018, 21:20 UTC
- Horário editado: 04 de novembro de 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "appsync.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/AWSServiceRoleForAppSync*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total de invocação ao serviço AppSync, tanto por meio do console quanto de forma independente

### A utilização desta política

Você pode vincular a AWSAppSyncInvokeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 20 de março de 2018, 21:21 UTC
- Horário editado: 20 de março de 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSAppSyncPushToCloudWatchLogs

AWSAppSyncPushToCloudWatchLogs é uma [política AWS gerenciada](#) que: Permite que o AppSync envie registros para a conta do CloudWatch do usuário.

## A utilização desta política

Você pode vincular a AWSAppSyncPushToCloudWatchLogs aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de abril de 2018, 19:38 UTC
- Horário editado: 09 de abril de 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor é uma [política AWS gerenciada](#) que: fornece acesso para criar, atualizar e consultar o esquema.

### A utilização desta política

Você pode vincular a AWSAppSyncSchemaAuthor aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de março de 2018, 21:21 UTC
- Horário editado: 01 de fevereiro de 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "appsync:GraphQL",
      "appsync:CreateResolver",
      "appsync:CreateType",
      "appsync>DeleteResolver",
      "appsync>DeleteType",
      "appsync:GetResolver",
      "appsync:GetType",
      "appsync:GetDataSource",
      "appsync:GetSchemaCreationStatus",
      "appsync:GetIntrospectionSchema",
      "appsync:GetGraphQLApi",
      "appsync:ListTypes",
      "appsync:ListApiKeys",
      "appsync:ListResolvers",
      "appsync:ListDataSources",
      "appsync:ListGraphQLApis",
      "appsync:StartSchemaCreation",
      "appsync:UpdateResolver",
      "appsync:UpdateType",
      "appsync:TagResource",
      "appsync:UntagResource",
      "appsync:ListTagsForResource",
      "appsync:CreateFunction",
      "appsync:UpdateFunction",
      "appsync:GetFunction",
      "appsync>DeleteFunction",
      "appsync:ListFunctions",
      "appsync:ListResolversByFunction",
      "appsync:EvaluateMappingTemplate",
      "appsync:EvaluateCode"
    ],
    "Resource" : "*"
  }
]
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso aos AWS serviços e recursos usados ou gerenciados pelo AppSync

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário da criação: 21 de janeiro de 2020, 19:56 UTC
- Horário editado: 21 de janeiro de 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingTargets",
      "xray:GetSamplingRules",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSArtifactAccountSync

AWSArtifactAccountSync é uma [política AWS gerenciada](#) que: Permite que o AWS Artifact tenha acesso somente de leitura às operações em Organizations. AWS

### A utilização desta política

Você pode vincular a AWSArtifactAccountSync aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 10 de abril de 2018, 23:04 UTC
- Horário editado: 10 de abril de 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSArtifactReportsReadOnlyAccess

AWSArtifactReportsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura aos relatórios do serviço AWS Artifact.

## Utilização desta política

Você pode vincular a `AWSArtifactReportsReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 02 de janeiro de 2024, 22:42 UTC
- Horário editado: 02 de janeiro de 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSArtifactServiceRolePolicy

AWSArtifactServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que a AWS Artifact colete informações sobre uma organização por meio do serviço AWS Organizations.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de agosto de 2023, 20:27 UTC
- Horário editado: 21 de agosto de 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess é uma [política AWS gerenciada](#) que: fornece acesso administrativo para ativar ou desativar o AWS Audit Manager, atualizar configurações e gerenciar avaliações, controles e estruturas

### A utilização desta política

Você pode vincular a AWSAuditManagerAdministratorAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de dezembro de 2020, 20:02 UTC

- Horário editado: 30 de abril de 2022, 00:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
```

```

    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "organizations:ServicePrincipal" : [
        "auditmanager.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "IAMAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser",
    "iam:ListUsers",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMAccessCreateSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "auditmanager.amazonaws.com"
    }
  }
},
{
  "Sid" : "IAMAccessManageSLR",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:UpdateRoleDescription",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],

```



```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
  },
  {
    "Sid" : "S3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      },
      "StringLike" : {
        "kms:ViaService" : "auditmanager.*.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SNSAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  }
```

```
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    }
  ],
  {
    "Sid" : "EventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "events>DeleteRule",
      "events:DescribeRule",
      "events:EnableRule",
      "events:DisableRule",
      "events>ListTargetsByRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  },
  {
    "Sid" : "TagAccess",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAuditManagerServiceRolePolicy

AWSAuditManagerServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS Audit Manager

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 08 de dezembro de 2020, 15:12 UTC
- Horário editado: 06 de dezembro de 2023, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "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:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "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:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:ListEntitiesForPolicy",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListOpenIdConnectProviders",
"iam:ListPolicies",
"iam:ListRolePolicies",
```

```
"iam:ListRoles",
"iam:ListSamlProviders",
"iam:ListUserPolicies",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"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",
"organizations:DescribeOrganization",
"organizations:DescribePolicy",
"rds:DescribeCertificates",
"rds:DescribeDbClusterEndpoints",
"rds:DescribeDbClusterParameterGroups",
"rds:DescribeDbClusters",
"rds:DescribeDBInstances",
"rds:DescribeDbSecurityGroups",
"redshift:DescribeClusters",
"route53:GetQueryLoggingConfig",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:ListAllMyBuckets",
"securityhub:DescribeStandards",
"sns:ListTopics",
"sqs:ListQueues",
"waf-regional:GetLoggingConfiguration",
"waf-regional:ListRuleGroups",
```

```
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
  ],
  "Resource" : "*",
  "Sid" : "AuditManagerAPICallAccess"
},
{
  "Sid" : "AuditManagerS3GetBucketPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketPolicy"
  ],
  "Resource" : "*",
  "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"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao AWS Auto Scaling para prever periodicamente a capacidade e gerar ações de escalabilidade programadas para grupos de Auto Scaling em um plano de escalabilidade

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de agosto de 2018, 22:46 UTC
- Horário editado: 23 de agosto de 2018, 22:46 UTC



- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSBackupAuditAccess

AWSBackupAuditAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões para que os usuários criem controles e estruturas que definam suas expectativas em relação aos recursos e atividades de AWS Backup e auditem os recursos e atividades de AWS Backup em relação aos controles e estruturas definidos. Essa política concede permissões ao AWS Config e serviços similares para descrever as expectativas do usuário e realizar as auditorias. Essa política também concede permissões para entregar relatórios de auditoria ao S3 e serviços similares e permite que os usuários encontrem e abram seus relatórios de auditoria.

## A utilização desta política

Você pode vincular a AWSBackupAuditAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de agosto de 2021, 01:02 UTC
- Horário editado: 10 de abril de 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "backup:ListFrameworks",
    "backup:DescribeFramework",
    "backup>DeleteFramework",
    "backup:ListBackupPlans",
    "backup:ListBackupVaults",
    "backup:CreateReportPlan",
    "backup:UpdateReportPlan",
    "backup:ListReportPlans",
    "backup:DescribeReportPlan",
    "backup>DeleteReportPlan",
    "backup:StartReportJob",
    "backup:ListReportJobs",
    "backup:DescribeReportJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus",
    "config:DescribeComplianceByConfigRule"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:GetComplianceDetailsByConfigRule"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource" : "arn:aws:s3:::*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupDataTransferAccess

`AWSBackupDataTransferAccess` é uma [política AWS gerenciada](#) que: Essa política permite que o agente AWS Backint conclua a transferência de dados de backup com o plano AWS Backint Storage. Vincule essa política às funções assumidas pelas instâncias do EC2 que executam o SAP HANA com o agente Backint.

### A utilização desta política

Você pode vincular a `AWSBackupDataTransferAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de novembro de 2022, 22:48 UTC
- Horário editado: 10 de novembro de 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "backup-storage:StartObject",
      "backup-storage:PutChunk",
      "backup-storage:GetChunk",
      "backup-storage:ListChunks",
      "backup-storage:ListObjects",
      "backup-storage:GetObjectMetadata",
      "backup-storage:NotifyObjectComplete"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupFullAccess

AWSBackupFullAccess é uma [política gerenciada pela AWS](#) que: Essa política é para administradores de backup, concedendo acesso total às operações de AWS backup, incluindo a criação ou edição de planos de backup, a atribuição de AWS recursos aos planos de backup, a exclusão de backups e a restauração de backups.

## Utilização desta política

Você pode vincular a AWSBackupFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 18 de novembro de 2019, 22:21 UTC
- Horário editado: 27 de novembro de 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

## Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
```

```

    "rds:describeOptionGroups",
    "rds:describeOrderableDBInstanceOptions",
    "rds:describeDBSubnetGroups",
    "rds:describeDBClusterSnapshots",
    "rds:describeDBClusters",
    "rds:describeDBParameterGroups",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RdsDeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:DeleteDBSnapshot",
    "rds:DeleteDBClusterSnapshot"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "backup.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DynamoDbPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:ListBackups",
    "dynamodb:ListTables"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DynamoDbDeleteBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DeleteBackup"
  ],
  "Resource" : "*"
}

```

```
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "backup.amazonaws.com"
    ]
  }
},
{
  "Sid" : "EfsFileSystemPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeFilesystems"
  ],
  "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
},
{
  "Sid" : "Ec2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:describeAvailabilityZones",
    "ec2:DescribeVpcs",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeAddresses"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2DeletePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSnapshot",
    "ec2:DeregisterImage"
  ],
  "Resource" : "*",
```



```
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "backup.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ResourceGroupTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetTagKeys",
      "tag:GetTagValues",
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "StorageGatewayVolumePermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeCachediSCSIVolumes",
      "storagegateway:DescribeStorediSCSIVolumes"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
  },
  {
    "Sid" : "StorageGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:ListGateways"
    ],
    "Resource" : "arn:aws:storagegateway:*:*:*"
  },
  {
    "Sid" : "StorageGatewayGatewayPermissions",
    "Effect" : "Allow",
    "Action" : [
      "storagegateway:DescribeGatewayInformation",
      "storagegateway: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" : "*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync é uma [política AWS gerenciada](#) que: Fornece permissão ao AWS BackupGateway para sincronizar os metadados das máquinas virtuais em seu nome

## A utilização desta política

Você pode vincular a AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 15 de dezembro de 2022, 19:43 UTC
- Horário editado: 15 de dezembro de 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSBackupOperatorAccess

AWSBackupOperatorAccess é uma [política AWS gerenciada](#) que: Essa política concede aos usuários permissões para atribuir AWS recursos aos planos de backup, criar backups sob demanda e restaurar backups. Essa política não permite que o usuário crie ou edite planos de backup ou exclua backups agendados após sua criação.

## A utilização desta política

Você pode vincular a AWSBackupOperatorAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de novembro de 2019, 22:23 UTC
- Horário editado: 06 de setembro de 2023, 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

## Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupOrganizationAdminAccess

AWSBackupOrganizationAdminAccess é uma [política AWS gerenciada](#) que: Essa política é para administradores de backup que usam o gerenciamento de backup entre contas para gerenciar backups para a organização.

### A utilização desta política

Você pode vincular a AWSBackupOrganizationAdminAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2020, 16:23 UTC

- Horário editado: 18 de novembro de 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
```

```
        "backup.amazonaws.com"
      ]
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:AttachPolicy",
      "organizations:ListPoliciesForTarget",
      "organizations:ListTargetsForPolicy",
      "organizations:DetachPolicy",
      "organizations:DisablePolicyType",
      "organizations:DescribePolicy",
      "organizations:DescribeEffectivePolicy",
      "organizations:ListPolicies",
      "organizations:EnablePolicyType",
      "organizations:CreatePolicy",
      "organizations:UpdatePolicy",
      "organizations>DeletePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "organizations:PolicyType" : [
          "BACKUP_POLICY"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListRoots",
      "organizations:ListParents",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListAccountsForParent",
      "organizations:ListAccounts",
      "organizations:DescribeOrganization",
      "organizations:ListOrganizationalUnitsForParent",
      "organizations:ListChildren",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganizationalUnit"
    ],
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA é uma [política AWS gerenciada](#) que: Fornece permissão de AWS backup para restaurar um backup do SAP HANA no Amazon EC2

### A utilização desta política

Você pode vincular a AWSBackupRestoreAccessForSAPHANA aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de novembro de 2022, 22:43 UTC
- Horário editado: 10 de novembro de 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceLinkedRolePolicyForBackup

AWSBackupServiceLinkedRolePolicyForBackup é uma [política gerenciada pela AWS](#) que: Fornece permissão AWS de Backup para criar backups em seu nome em todos AWS os serviços

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de junho de 2020, 23:08 UTC
- Horário editado: 15 de dezembro de 2023, 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

### Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "elasticfilesystem:Backup",
  "elasticfilesystem:DescribeTags"
],
"Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
  }
}
},
{
  "Sid" : "DescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources",
    "elasticfilesystem:DescribeFileSystems",
    "dynamodb:ListTables",
    "storagegateway:ListVolumes",
    "ec2:DescribeVolumes",
    "ec2:DescribeInstances",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnapshotCopyTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
}
},
{
  "Sid" : "EC2CreateBackupTagPermissions",
```

```
"Effect" : "Allow",
"Action" : "ec2:CreateTags",
"Resource" : [
  "arn:aws:ec2:*::image/*",
  "arn:aws:ec2:*::snapshot/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AWSBackupManagedResource"
    ]
  }
}
},
{
  "Sid" : "EC2CreateTagsPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSBackupManagedResource" : "false"
    }
  }
},
{
  "Sid" : "EC2RDSDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeImages",
    "rds:DescribeDBSnapshots",
    "rds:DescribeDBClusterSnapshots"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EBSCopyPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CopySnapshot",
```



```

    "Resource" : "arn:aws:ec2:*:*:snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopyImage",
    "Resource" : "*"
  },
  {
    "Sid" : "EC2ModifyPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeregisterImage",
      "ec2>DeleteSnapshot",
      "ec2:ModifySnapshotTier"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  },
  {
    "Sid" : "RDSInstanceAndSnashotPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:AddTagsToResource",
      "rds:CopyDBSnapshot",
      "rds>DeleteDBSnapshot",
      "rds>DeleteDBInstanceAutomatedBackup"
    ],
    "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
  },
  {
    "Sid" : "RDSClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "rds:AddTagsToResource",
      "rds:CopyDBClusterSnapshot",
      "rds>DeleteDBClusterSnapshot"
    ],
    "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
  },

```

```
{
  "Sid" : "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/*"
  ]
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceLinkedRolePolicyForBackupTest

AWSBackupServiceLinkedRolePolicyForBackupTest é uma [política AWS gerenciada](#) que: Fornece permissão AWS de Backup para criar backups em seu nome em todos AWS os serviços

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de maio de 2020, 17:37 UTC

- Horário editado: 12 de maio de 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceRolePolicyForBackup

AWSBackupServiceRolePolicyForBackup é uma [política gerenciada pela AWS](#) que: Fornece permissão AWS de Backup para criar backups em seu nome em todos AWS os serviços

### Utilização desta política

Você pode vincular a AWSBackupServiceRolePolicyForBackup aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 10 de janeiro de 2019, 21:01 UTC
- Horário editado: 15 de dezembro de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

### Versão da política

Versão da política: v18 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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



```
{
  "Sid" : "DynamoDBPermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DescribeTable",
    "dynamodb:CreateBackup"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*"
},
{
  "Sid" : "DynamoDBBackupResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:DescribeBackup",
    "dynamodb>DeleteBackup"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
},
{
  "Sid" : "DynamoDBBackupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:ListTagsForResource",
    "rds:DescribeDBSnapshots",
    "rds:CreateDBSnapshot",
    "rds:CopyDBSnapshot",
    "rds:DescribeDBInstances",
    "rds:CreateDBClusterSnapshot",
    "rds:DescribeDBClusters",
    "rds:DescribeDBClusterSnapshots",
    "rds:CopyDBClusterSnapshot",
    "rds:DescribeDBClusterAutomatedBackups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "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" : "KMSDataKeyEC2Permissions",
    "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" : "SSMSAPPPermissions",

```

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceRolePolicyForRestores

`AWSBackupServiceRolePolicyForRestores` é uma [política gerenciada pela AWS](#) que: Fornece permissão de AWS Backup para realizar restaurações em seu nome em todos AWS os serviços. Essa política inclui permissões para criar e excluir AWS recursos, como volumes do EBS, instâncias do RDS e sistemas de arquivos EFS, que fazem parte do processo de restauração.

## Utilização desta política

Você pode vincular a `AWSBackupServiceRolePolicyForRestores` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 12 de janeiro de 2019, 00:23 UTC
- Horário editado: 15 de dezembro de 2023, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

## Versão da política

Versão da política: v20 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb>DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    }
  ]
}
```

```
},
{
  "Sid" : "DynamoDBBackupResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:RestoreTableFromBackup"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
},
{
  "Sid" : "EBSPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume",
    "ec2>DeleteVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "EC2DescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeVolumes",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSnapshotTierStatus"
  ],
  "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" : [
    "*"
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup é uma [política AWS gerenciada](#) que: Política contendo as permissões necessárias para o AWS Backup fazer backup de dados em qualquer bucket do S3. Isso inclui acesso de leitura a todos os objetos do S3 e qualquer acesso de descryptografia para todas as chaves do KMS.

### A utilização desta política

Você pode vincular a AWSBackupServiceRolePolicyForS3Backup aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de fevereiro de 2022, 17:40 UTC

- Horário editado: 01 de setembro de 2022, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
},
{
  "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:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectAcl",
    "s3:GetObject",
    "s3:GetObjectVersionTagging",
    "s3:GetObjectVersionAcl",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::*/*"
},
{
  "Effect" : "Allow",
  "Action" : "s3:ListAllMyBuckets",
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore é uma [política AWS gerenciada](#) que: Política contendo as permissões necessárias para que o AWS Backup restaure um backup do S3 em um bucket. Isso inclui permissões de leitura/gravação em todos os buckets do S3 e permissões para GenerateDataKey e DescribeKey para todas as chaves KMS.

## A utilização desta política

Você pode vincular a AWSBackupServiceRolePolicyForS3Restore aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de fevereiro de 2022, 17:39 UTC
- Horário editado: 07 de fevereiro de 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3::*/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBatchFullAccess

AWSBatchFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do AWS Batch.

### A utilização desta política

Você pode vincular a AWSBatchFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de dezembro de 2016, 19:35 UTC

- Horário editado: 24 de outubro de 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSBatchServiceEventTargetRole

AWSBatchServiceEventTargetRole é uma [política AWS gerenciada que: Política](#) para habilitar o CloudWatch Event Target for Batch AWS Job Submission

## A utilização desta política

Você pode vincular a AWSBatchServiceEventTargetRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 28 de fevereiro de 2018, 22:31 UTC
- Horário editado: 28 de fevereiro de 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBatchServiceRole

`AWSBatchServiceRole` é uma [política gerenciada pela AWS](#) que: função de serviço Policy for AWS Batch que permite acesso a serviços relacionados, incluindo EC2, Autoscaling, serviço de contêiner EC2 e Cloudwatch Logs.

### Utilização desta política

Você pode vincular a `AWSBatchServiceRole` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 06 de dezembro de 2016, 19:36 UTC
- Horário editado: 05 de dezembro de 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

### Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "AWSBatchPolicyStatement1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeImages",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeSpotInstanceRequests",
      "ec2:DescribeSpotFleetInstances",
      "ec2:DescribeSpotFleetRequests",
      "ec2:DescribeSpotPriceHistory",
      "ec2:DescribeSpotFleetRequestHistory",
      "ec2:DescribeVpcClassicLink",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:CreateLaunchTemplate",
      "ec2>DeleteLaunchTemplate",
      "ec2:RequestSpotFleet",
      "ec2:CancelSpotFleetRequests",
      "ec2:ModifySpotFleetRequest",
      "ec2:TerminateInstances",
      "ec2:RunInstances",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeLaunchConfigurations",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeScalingActivities",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:SetDesiredCapacity",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling:SuspendProcesses",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "ecs:DescribeClusters",
```



```

    "ecs:DescribeContainerInstances",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTasks",
    "ecs:ListAccountSettings",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "ecs:ListTasks",
    "ecs:CreateCluster",
    "ecs>DeleteCluster",
    "ecs:RegisterTaskDefinition",
    "ecs:DeregisterTaskDefinition",
    "ecs:RunTask",
    "ecs:StartTask",
    "ecs:StopTask",
    "ecs:UpdateContainerAgent",
    "ecs:DeregisterContainerInstance",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : "ecs:TagResource",
  "Resource" : [
    "arn:aws:ecs:*:*:task/*_Batch_*"
  ]
},
{
  "Sid" : "AWSBatchPolicyStatement3",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
    "iam:PassedToService" : [
      "ec2.amazonaws.com",
      "ec2.amazonaws.com.cn",
      "ecs-tasks.amazonaws.com"
    ]
  }
},
{
  "Sid" : "AWSBatchPolicyStatement4",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "autoscaling.amazonaws.com",
        "ecs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement5",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBillingConductorFullAccess

`AWSBillingConductorFullAccess` é uma [política AWS gerenciada que: Use a política gerenciada](#) `AWSBillingConductorFullAccess` para permitir acesso completo ao console (ABC) e às AWS Billing Conductor APIs. Essa política permite que os usuários listem, criem e excluam recursos ABC.

### A utilização desta política

Você pode vincular a `AWSBillingConductorFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de abril de 2022, 18:02 UTC
- Horário editado: 13 de abril de 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBillingConductorReadOnlyAccess

`AWSBillingConductorReadOnlyAccess` é uma [política AWS gerenciada que: Use a política gerenciada `AWSBillingConductorReadOnlyAccess`](#) para permitir acesso somente de leitura ao console (ABC) e às APIs. AWS Billing Conductor Essa política concede permissão para obter e listar todos os recursos do IAM. A política não inclui a capacidade de criar ou excluir recursos.

### A utilização desta política

Você pode vincular a `AWSBillingConductorReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de abril de 2022, 18:02 UTC
- Horário editado: 13 de abril de 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess é uma [política gerenciada pela AWS](#) que: permite que os usuários visualizem as faturas no Billing Console.

### Utilização desta política

Você pode vincular a AWSBillingReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 27 de agosto de 2020, 20:08 UTC
- Horário editado: 17 de janeiro de 2024, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
```

```
"billing:GetBillingDetails",
"billing:GetBillingNotifications",
"billing:GetBillingPreferences",
"billing:GetCredits",
"billing:GetContractInformation",
"billing:GetIAMAccessPreference",
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"budgets:ViewBudget",
"budgets:DescribeBudgetActionsForBudget",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionHistories",
"ce:DescribeCostCategoryDefinition",
"ce:GetCostAndUsage",
"ce:ListCostCategoryDefinitions",
"ce:ListTagsForResource",
"ce:ListCostAllocationTags",
"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",
" purchase-orders:GetPurchaseOrder",
" purchase-orders:ViewPurchaseOrders",
" purchase-orders:ListPurchaseOrderInvoices",
" purchase-orders:ListPurchaseOrders",
" purchase-orders:ListTagsForResource",
" sustainability:GetCarbonFootprintSummary",
" tax:GetTaxRegistrationDocument",
" tax:GetTaxInheritance",
" tax:ListTaxRegistrations"
],
"Resource" : "*"
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBudgetsActions\_RolePolicyForResourceAdministrationWithSSM

AWSBudgetsActions\_RolePolicyForResourceAdministrationWithSSM é uma [política AWS gerenciada](#) que: Essa política dá permissões para controlar AWS recursos. Por exemplo, ela inicia e interrompe instâncias do EC2 ou do RDS ao executar scripts do AWS Systems Manager (SSM).

## A utilização desta política

Você pode vincular a AWSBudgetsActions\_RolePolicyForResourceAdministrationWithSSM aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de maio de 2022, 19:03 UTC
- Horário editado: 25 de maio de 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

## Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total às ações de AWS orçamentos, incluindo o uso de ações de orçamentos para controlar os estados de execução dos recursos por meio de AWS AWS Management Console

### A utilização desta política

Você pode vincular a `AWSBudgetsActionsWithAWSResourceControlAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de outubro de 2020, 17:19 UTC
- Horário editado: 15 de outubro de 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
```

```
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBudgetsReadOnlyAccess

AWSBudgetsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao AWS Budgets Console por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSBudgetsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de outubro de 2020, 17:18 UTC
- Horário editado: 15 de outubro de 2020, 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBugBustFullAccess

AWSBugBustFullAccess é uma [política AWS gerenciada](#) que: Essa política do IAM concede aos usuários acesso total ao console do AWS BugBust

## A utilização desta política

Você pode vincular a AWSBugBustFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2021, 07:03 UTC
- Horário editado: 22 de julho de 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    }
  ],
  {
```

```
    "Sid" : "AWSBugBustFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "bugbust:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSBugBustSLRCreation",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "bugbust.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBugBustPlayerAccess

AWSBugBustPlayerAccess é uma [política AWS gerenciada](#) que: Essa política do IAM concede aos usuários acesso para participar de eventos do AWS BugBust

## A utilização desta política

Você pode vincular a AWSBugBustPlayerAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2021, 07:15 UTC
- Horário editado: 24 de junho de 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
```



```
"Action" : [
  "bugbust:ListBugs",
  "bugbust:ListProfilingGroups",
  "bugbust:JoinEvent",
  "bugbust:GetEvent",
  "bugbust:ListEvents",
  "bugbust:GetJoinEventStatus",
  "bugbust:ListEventScores",
  "bugbust:ListEventParticipants",
  "bugbust:UpdateWorkItem",
  "bugbust:ListPullRequests"
],
"Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede permissões ao AWS BugBust para acessar recursos em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de junho de 2021, 06:59 UTC

- Horário editado: 24 de junho de 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Certificate Manager (ACM)

## A utilização desta política

Você pode vincular a AWSCertificateManagerFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de janeiro de 2016, 17:02 UTC
- Horário editado: 17 de agosto de 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "acm.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus",
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerPrivateCAAuditor

AWSCertificateManagerPrivateCAAuditor é uma [política AWS gerenciada](#) que: Fornece acesso de auditor à Autoridade de Certificação Privada do AWS Certificate Manager

## A utilização desta política

Você pode vincular a AWSCertificateManagerPrivateCAAuditor aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 23 de outubro de 2018, 16:51 UTC
- Horário editado: 17 de agosto de 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
    }
  ]
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerPrivateCAFullAccess

AWSCertificateManagerPrivateCAFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à Autoridade de AWS Certificação Privada do Certificate Manager

### A utilização desta política

Você pode vincular a AWSCertificateManagerPrivateCAFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 23 de outubro de 2018, 16:54 UTC
- Horário editado: 23 de outubro de 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerPrivateCAPrivilegedUser

AWSCertificateManagerPrivateCAPrivilegedUser é uma [política AWS gerenciada](#) que: Fornece acesso privilegiado de usuários certificados à Autoridade de AWS Certificação Privada do Certificate Manager

### A utilização desta política

Você pode vincular a AWSCertificateManagerPrivateCAPrivilegedUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de junho de 2019, 17:43 UTC

- Horário editado: 20 de junho de 2019, 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerPrivateCAReadOnly

AWSCertificateManagerPrivateCAReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura à Autoridade de AWS Certificação Privada do Certificate Manager

## A utilização desta política

Você pode vincular a AWSCertificateManagerPrivateCAReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 23 de outubro de 2018, 16:57 UTC
- Horário editado: 17 de agosto de 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerPrivateCAUser

AWSCertificateManagerPrivateCAUser é uma [política AWS gerenciada](#) que: Fornece ao usuário certificado acesso à Autoridade de AWS Certificação Privada do Certificate Manager

### A utilização desta política

Você pode vincular a AWSCertificateManagerPrivateCAUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 23 de outubro de 2018, 16:53 UTC
- Horário editado: 20 de junho de 2019, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCertificateManagerReadOnly

AWSCertificateManagerReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS Certificate Manager (ACM).

### A utilização desta política

Você pode vincular a AWSCertificateManagerReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de janeiro de 2016, 17:07 UTC
- Horário editado: 15 de março de 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : {
  "Effect" : "Allow",
  "Action" : [
    "acm:DescribeCertificate",
    "acm:ListCertificates",
    "acm:GetCertificate",
    "acm:ListTagsForCertificate",
    "acm:GetAccountConfiguration"
  ],
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSChatbotServiceLinkedRolePolicy

AWSChatbotServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: A função vinculada ao serviço usada pelo AWS Chatbot.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de novembro de 2019, 16:39 UTC
- Horário editado: 18 de novembro de 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCleanRoomsFullAccess

AWSCleanRoomsFullAccess é uma [política AWS gerenciada](#) que: Permite acesso total aos recursos da Sala AWS Limpa e acesso a recursos relacionados Serviços da AWS.

### Utilização desta política

Você pode vincular a AWSCleanRoomsFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 12 de janeiro de 2023, 16:10 UTC
- Horário editado: 21 de março de 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

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



```
  },
  {
    "Sid" : "PassServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ListRolesToPickServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:ListRolePolicies",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
  },
  {
    "Sid" : "ListPoliciesToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "GetPolicyToInspectServiceRolePolicy",
    "Effect" : "Allow",
    "Action" : [
```

```
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
},
{
  "Sid" : "ConsoleDisplayTables",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsolePickQueryResultsBucketListAll",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SetQueryResultsBucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucketVersions"
  ],
  "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
},
{
  "Sid" : "WriteQueryResults",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:PutObject"
  ]
}
```

```
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleDisplayQueryResults",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
    "Sid" : "EstablishLogDeliveries",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:GetLogDelivery",
      "logs:UpdateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:ListLogDeliveries"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsDescribe",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "SetupLogGroupsCreate",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsResourcePolicy",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeResourcePolicies",
      "logs:PutResourcePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  }
}
```

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSCleanRoomsFullAccessNoQuerying

AWSCleanRoomsFullAccessNoQuerying é uma [política AWS gerenciada](#) que: Permite acesso total aos recursos da AWS Clean Rooms, exceto para consultas em uma colaboração e acesso a informações relacionadas Serviços da AWS.

### A utilização desta política

Você pode vincular a AWSCleanRoomsFullAccessNoQuerying aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2023, 16:12 UTC
- Horário editado: 31 de julho de 2023, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSCleanRoomsMLFullAccess

AWSCleanRoomsMLFullAccess é uma [política AWS gerenciada](#) que: Permite acesso total aos recursos de ML do AWS Clean Rooms e acesso a recursos relacionados Serviços da AWS.

## Utilização desta política

Você pode vincular a AWSCleanRoomsMLFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 29 de novembro de 2023, 21:02 UTC
- Horário editado: 29 de novembro de 2023, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
```

```

    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/cleanrooms-ml*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CleanRoomsConsoleNavigation",
    "Effect" : "Allow",
    "Action" : [
      "cleanrooms:GetCollaboration",
      "cleanrooms: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*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccess é uma [política AWS gerenciada](#) que: Permite acesso somente leitura aos recursos de ML do AWS Clean Rooms e acesso somente leitura aos recursos relacionados do Clean Rooms AWS

### Utilização desta política

Você pode vincular a AWSCleanRoomsMLReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 29 de novembro de 2023, 20:55 UTC
- Horário editado: 29 de novembro de 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCleanRoomsReadOnlyAccess

`AWSCleanRoomsReadOnlyAccess` é uma [política AWS gerenciada](#) que: Permite acesso somente para leitura aos recursos do AWS Clean Rooms e acesso somente para leitura aos recursos relacionados do AWS Glue e do Amazon CloudWatch Logs.

### A utilização desta política

Você pode vincular a `AWSCleanRoomsReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de janeiro de 2023, 16:10 UTC
- Horário editado: 12 de janeiro de 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CleanRoomsRead",
    "Effect" : "Allow",
    "Action" : [
      "cleanrooms:BatchGet*",
      "cleanrooms:Get*",
      "cleanrooms:List*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleDisplayTables",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:GetSchema",
      "glue:GetSchemaVersion",
      "glue:BatchGetPartition"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  }
]
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloud9Administrator

AWSCloud9Administrator é uma [política AWS gerenciada](#) que: Fornece acesso de administrador ao AWS Cloud9.

### A utilização desta política

Você pode vincular a AWSCloud9Administrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:17 UTC
- Horário editado: 11 de outubro de 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloud9EnvironmentMember

AWSCloud9EnvironmentMember é uma [política AWS gerenciada](#) que: Fornece a capacidade de ser convidado para os ambientes de desenvolvimento AWS compartilhados do Cloud9.

### A utilização desta política

Você pode vincular a AWSCloud9EnvironmentMember aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:18 UTC
- Horário editado: 11 de outubro de 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloud9ServiceRolePolicy

AWSCloud9ServiceRolePolicy é uma [política AWS gerenciada](#) que: Service Linked Role Policy for AWS Cloud9

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de novembro de 2017, 13:44 UTC
- Horário editado: 17 de janeiro de 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```



```

    "ec2:TerminateInstances",
    "ec2>DeleteSecurityGroup",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/Name" : "aws-cloud9-*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [

```

```
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : [
    "arn:aws:license-manager:*:*:license-configuration:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:instance-profile/cloud9/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/AWSCloud9SSMAccessRole"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSCloud9SSMInstanceProfile

AWSCloud9SSMInstanceProfile é uma [política AWS gerenciada](#) que: Essa política será usada para anexar uma função em um InstanceProfile, o que permitirá que o Cloud9 use o SSM Session Manager para se conectar à instância

## A utilização desta política

Você pode vincular a AWSCloud9SSMInstanceProfile aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de maio de 2020, 11:40 UTC
- Horário editado: 14 de maio de 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloud9User

AWSCloud9User é uma [política gerenciada da AWS](#) que: Fornece permissão para criar AWS ambientes de desenvolvimento Cloud9.

## A utilização desta política

Você pode vincular a AWSCloud9User aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de novembro de 2017, 16:16 UTC
- Horário editado: 11 de outubro de 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudFormationFullAccess

AWSCloudFormationFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CloudFormation.

### A utilização desta política

Você pode vincular a AWSCloudFormationFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de julho de 2019, 21:50 UTC
- Horário editado: 26 de julho de 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudFormationReadOnlyAccess

AWSCloudFormationReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso ao AWS CloudFormation por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a AWSCloudFormationReadOnlyAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 13 de novembro de 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudFrontLogger

AWSCloudFrontLogger é uma [política AWS gerenciada](#) que: Concede permissões de gravação ao CloudFront Logger para o CloudWatch Logs.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de junho de 2018, 20:15 UTC
- Horário editado: 22 de novembro de 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudHSMFullAccess

AWSCloudHSMFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total a todos os recursos do CloudHSM.

### A utilização desta política

Você pode vincular a AWSCloudHSMFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudHSMReadOnlyAccess

AWSCloudHSMReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todos os recursos do CloudHSM.

### A utilização desta política

Você pode vincular a AWSCloudHSMReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudHSMRole

`AWSCloudHSMRole` é uma [política AWS gerenciada que: Política](#) padrão para a função de serviço AWS CloudHSM.

## A utilização desta política

Você pode vincular a `AWSCloudHSMRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudMapDiscoverInstanceAccess

AWSCloudMapDiscoverInstanceAccess é uma [política AWS gerenciada](#) que: Fornece acesso à API de descoberta de Nuvem AWS mapas.

### A utilização desta política

Você pode vincular a AWSCloudMapDiscoverInstanceAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2018, 00:02 UTC
- Horário editado: 20 de setembro de 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudMapFullAccess

AWSCloudMapFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as ações do Nuvem AWS Mapa.

### A utilização desta política

Você pode vincular a AWSCloudMapFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS



- Hora de criação: 28 de novembro de 2018, 23:57 UTC
- Horário editado: 29 de julho de 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53>DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudMapReadOnlyAccess

`AWSCloudMapReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura a todas as ações do Nuvem AWS Mapa.

### A utilização desta política

Você pode vincular a `AWSCloudMapReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 28 de novembro de 2018, 23:45 UTC
- Horário editado: 20 de setembro de 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudMapRegisterInstanceAccess

AWSCloudMapRegisterInstanceAccess é uma [política AWS gerenciada](#) que: Fornece acesso em nível de registrante às ações do Nuvem AWS Map.

### A utilização desta política

Você pode vincular a AWSCloudMapRegisterInstanceAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 29 de novembro de 2018, 00:04 UTC
- Horário editado: 20 de setembro de 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53>DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudShellFullAccess

AWSCloudShellFullAccess é uma [política AWS gerenciada](#) que: Concede o uso do AWS CloudShell com todos os recursos

### A utilização desta política

Você pode vincular a AWSCloudShellFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 18:07 UTC
- Horário editado: 15 de dezembro de 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "cloudshell:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudTrail\_FullAccess

AWSCloudTrail\_FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CloudTrail.

### A utilização desta política

Você pode vincular a `AWSCloudTrail_FullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de outubro de 2020, 23:41 UTC
- Horário editado: 22 de fevereiro de 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3::*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
```

```
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "cloudtrail:*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "iam:GetRolePolicy",
    "iam:GetUser"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "cloudtrail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateKey",
```



```
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "lambda:ListFunctions"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudTrail\_ReadOnlyAccess

AWSCloudTrail\_ReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao AWS CloudTrail.

### A utilização desta política

Você pode vincular a AWSCloudTrail\_ReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de junho de 2022, 17:19 UTC
- Horário editado: 14 de junho de 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCloudWatchAlarms\_ActionSSMIncidentsServiceRolePolicy

AWSCloudWatchAlarms\_ActionSSMIncidentsServiceRolePolicy é uma [política AWS gerenciada que: Essa política](#) é usada pela função vinculada ao serviço chamada AWSServiceRoleForCloudWatchAlarms\_ActionsMIncidents. O CloudWatch usa essa função vinculada ao serviço para AWS executar ações do System Manager Incident Manager quando o alarme do CloudWatch passa para o estado ALARM. Esta política concede permissão para iniciar incidentes em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de abril de 2021, 13:30 UTC
- Horário editado: 27 de abril de 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Sid" : "StartIncidentPermissions",
  "Effect" : "Allow",
  "Action" : "ssm-incidents:StartIncident",
  "Resource" : "*"
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeArtifactAdminAccess

AWSCodeArtifactAdminAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CodeArtifact por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSCodeArtifactAdminAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de junho de 2020, 23:53 UTC
- Horário editado: 16 de junho de 2020, 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeArtifactReadOnlyAccess

AWSCodeArtifactReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS CodeArtifact por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a `AWSCodeArtifactReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de junho de 2020, 21:23 UTC
- Horário editado: 25 de junho de 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
        "sts:AWSServiceName" : "codeartifact.amazonaws.com"
    }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CodeBuild por meio do. AWS Management Console Além disso, anexe AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de compilação e anexe IAMFullAccess para criar e gerenciar a função de serviço do CodeBuild.

## A utilização desta política

Você pode vincular a AWSCodeBuildAdminAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2016, 19:04 UTC
- Horário editado: 31 de julho de 2023, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

## Versão da política

Versão da política: v13 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
```



```
"Action" : [
  "logs:DeleteLogGroup"
],
"Effect" : "Allow",
"Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:CreateConnection",
    "codestar-connections>DeleteConnection",
    "codestar-connections:UpdateConnectionInstallation",
    "codestar-connections:TagResource",
    "codestar-connections:UntagResource",
    "codestar-connections:ListConnections",
    "codestar-connections:ListInstallationTargets",
    "codestar-connections:ListTagsForResource",
    "codestar-connections:GetConnection",
    "codestar-connections:GetIndividualAccessToken",
    "codestar-connections:GetInstallationUrl",
    "codestar-connections:PassConnection",
    "codestar-connections:StartOAuthHandshake",
    "codestar-connections:UseConnection"
  ],
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
},
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess é uma [política AWS gerenciada](#) que: Fornece acesso ao AWS CodeBuild por meio AWS Management Console do, mas não permite a administração do projeto CodeBuild. Anexe também o AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de compilação.

## A utilização desta política

Você pode vincular a AWSCodeBuildDeveloperAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2016, 19:02 UTC
- Horário editado: 31 de julho de 2023, 23:06 UTC

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

## Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "SSMParameterWriteAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
  },
  {
    "Sid" : "SSMStartSessionAccess",
    "Effect" : "Allow",
    "Action" : [
      "ssm:StartSession"
    ],
    "Resource" : "arn:aws:ecs:*:*:task/*/*"
  },
  {
    "Sid" : "CodeStarConnectionsUserAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:ListConnections",
      "codestar-connections:GetConnection"
    ],
    "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
  },
  {
    "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"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSCodeBuildReadOnlyAccess

AWSCodeBuildReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS CodeBuild por meio do. AWS Management Console Anexe também o AmazonS3ReadOnlyAccess para fornecer acesso ao download de artefatos de compilação.

## A utilização desta política

Você pode vincular a AWSCodeBuildReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2016, 19:03 UTC
- Horário editado: 14 de setembro de 2020, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "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/*"
},
{
  "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"
}

```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeCommitFullAccess

AWSCodeCommitFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CodeCommit por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSCodeCommitFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:02 UTC
- Horário editado: 17 de julho de 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "codecommit:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:DisableRule",
    "events:EnableRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codecommit*"
},
{
  "Sid" : "SNSTopicAndSubscriptionReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
}
```

```
{
  "Sid" : "LambdaReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListUsers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyConsoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAccessKeys",
    "iam:ListSSHPublicKeys",
    "iam:ListServiceSpecificCredentials"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMUserSSHKeys",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSSHPublicKey",
    "iam:GetSSHPublicKey",
    "iam:ListSSHPublicKeys",
    "iam:UpdateSSHPublicKey",
    "iam:UploadSSHPublicKey"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMSelfManageServiceSpecificCredentials",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceSpecificCredential",
    "iam:UpdateServiceSpecificCredential",
```

```
    "iam:DeleteServiceSpecificCredential",
    "iam:ResetServiceSpecificCredential"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "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/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeCommitPowerUser

AWSCodeCommitPowerUser é uma [política AWS gerenciada](#) que: fornece acesso total aos repositórios do AWS CodeCommit, mas não permite a exclusão do repositório.

### A utilização desta política

Você pode vincular a AWSCodeCommitPowerUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:06 UTC
- Horário editado: 17 de julho de 2023, 21:49 UTC

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

## Versão da política

Versão da política: v15 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit>DeleteBranch",
        "codecommit>DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:DescribeRule",
      "events:DisableRule",
      "events:EnableRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/codecommit*"
  },
  {
    "Sid" : "SNSTopicAndSubscriptionAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:Subscribe",
      "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:codecommit*"
  },
  {
    "Sid" : "SNSTopicAndSubscriptionReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics",
      "sns:ListSubscriptionsByTopic",
      "sns:GetTopicAttributes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "LambdaReadOnlyListAccess",
    "Effect" : "Allow",
    "Action" : [
      "lambda:ListFunctions"
    ],
    "Resource" : "*"
  },
}
```



```
{
  "Sid" : "IAMReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListUsers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyConsoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAccessKeys",
    "iam:ListSSHPublicKeys",
    "iam:ListServiceSpecificCredentials"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMUserSSHKeys",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSSHPublicKey",
    "iam:GetSSHPublicKey",
    "iam:ListSSHPublicKeys",
    "iam:UpdateSSHPublicKey",
    "iam:UploadSSHPublicKey"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "IAMSelfManageServiceSpecificCredentials",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceSpecificCredential",
    "iam:UpdateServiceSpecificCredential",
    "iam>DeleteServiceSpecificCredential",
    "iam:ResetServiceSpecificCredential"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
```

```

    "Action" : [
      "codestar-notifications:CreateNotificationRule",
      "codestar-notifications:DescribeNotificationRule",
      "codestar-notifications:UpdateNotificationRule",
      "codestar-notifications:Subscribe",
      "codestar-notifications:Unsubscribe"
    ],
    "Resource" : "*",
    "Condition" : {
      "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/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeCommitReadOnly

AWSCodeCommitReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS CodeCommit por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSCodeCommitReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:05 UTC
- Horário editado: 18 de agosto de 2021, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "codecommit:BatchGet*",
    "codecommit:BatchDescribe*",
    "codecommit:Describe*",
    "codecommit:EvaluatePullRequestApprovalRules",
    "codecommit:Get*",
    "codecommit:List*",
    "codecommit:GitPull"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DescribeRule",
    "events:ListTargetsByRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/codecommit*"
},
{
  "Sid" : "SNSSubscriptionAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:ListFunctions"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyListAccess",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iam:ListUsers"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMReadOnlyConsoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListSSHPublicKeys",
    "iam:ListServiceSpecificCredentials",
    "iam:ListAccessKeys",
    "iam:GetSSHPublicKey"
  ],
  "Resource" : "arn:aws:iam::*:user/${aws:username}"
},
{
  "Sid" : "CodeStarConnectionsReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:ListConnections",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "arn:aws:codestar-connections::*:connection/*"
},
{
  "Sid" : "CodeStarNotificationsReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:DescribeNotificationRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "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" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess é uma [política AWS gerenciada](#) que: Fornece acesso para registrar e implantar uma revisão.

### A utilização desta política

Você pode vincular a AWSCodeDeployDeployerAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de maio de 2015, 18:18 UTC

- Horário editado: 02 de abril de 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSCodeDeployFullAccess

AWSCodeDeployFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do CodeDeploy.

## A utilização desta política

Você pode vincular a AWSCodeDeployFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de maio de 2015, 18:13 UTC
- Horário editado: 02 de abril de 2020, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
```

```
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "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" : "*"   
}   
]   
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployReadOnlyAccess

AWSCodeDeployReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do CodeDeploy.

### A utilização desta política

Você pode vincular a AWSCodeDeployReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de maio de 2015, 18:21 UTC
- Horário editado: 02 de abril de 2020, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRole

`AWSCodeDeployRole` é uma [política AWS gerenciada](#) que: Fornece acesso ao serviço CodeDeploy para expandir tags e interagir com o Auto Scaling em seu nome.

### A utilização desta política

Você pode vincular a `AWSCodeDeployRole` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 04 de maio de 2015, 18:05 UTC
- Horário editado: 16 de agosto de 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CompleteLifecycleAction",
      "autoscaling>DeleteLifecycleHook",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeLifecycleHooks",
      "autoscaling:PutLifecycleHook",
      "autoscaling:RecordLifecycleActionHeartbeat",
      "autoscaling>CreateAutoScalingGroup",
      "autoscaling>CreateOrUpdateTags",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:EnableMetricsCollection",
      "autoscaling:DescribePolicies",
      "autoscaling:DescribeScheduledActions",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:SuspendProcesses",
      "autoscaling:ResumeProcesses",
      "autoscaling:AttachLoadBalancers",
      "autoscaling:AttachLoadBalancerTargetGroups",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:PutWarmPool",
      "autoscaling:DescribeScalingActivities",
      "autoscaling>DeleteAutoScalingGroup",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:TerminateInstances",
      "tag:GetResources",
      "sns:Publish",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:PutMetricAlarm",
      "elasticloadbalancing:DescribeLoadBalancerAttributes",
      "elasticloadbalancing:DescribeTargetGroupAttributes",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeInstanceHealth",
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
      "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:RegisterTargets",
```

```
    "elasticloadbalancing:DeregisterTargets"  
  ],  
  "Resource" : "*" }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRoleForCloudFormation

AWSCodeDeployRoleForCloudFormation é uma [política AWS gerenciada](#) que: Fornece acesso ao serviço CodeDeploy para invocar a função Lambda em seu nome para realizar a implantação azul/verde por meio do CloudFormation.

### A utilização desta política

Você pode vincular a AWSCodeDeployRoleForCloudFormation aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de maio de 2020, 17:12 UTC
- Horário editado: 19 de maio de 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRoleForECS

`AWSCodeDeployRoleForECS` é uma [política AWS gerenciada](#) que: Fornece acesso amplo ao serviço CodeDeploy para realizar uma implantação azul/verde do ECS em seu nome. Concede acesso total aos serviços de suporte, como acesso total para ler todos os objetos do S3, invocar todas as funções do Lambda, publicar em todos os tópicos do SNS na conta e atualizar todos os serviços do ECS.

## A utilização desta política

Você pode vincular a `AWSCodeDeployRoleForECS` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 20:40 UTC
- Horário editado: 23 de setembro de 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs>DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ],
}
```

```
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ecs-tasks.amazonaws.com"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRoleForECSLimited

AWSCodeDeployRoleForECSLimited é uma [política AWS gerenciada](#) que: Fornece acesso limitado ao serviço CodeDeploy para realizar uma implantação azul/verde do ECS em seu nome.

### A utilização desta política

Você pode vincular a AWSCodeDeployRoleForECSLimited aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 20:42 UTC
- Horário editado: 23 de setembro de 2019, 22:10 UTC

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

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs>DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",

```

```
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    },
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam:*:role/ecsTaskExecutionRole",
      "arn:aws:iam:*:role/ECSTaskExecution*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambda é uma [política AWS gerenciada](#) que: Fornece acesso ao serviço CodeDeploy para realizar uma implantação do Lambda em seu nome.

### A utilização desta política

Você pode vincular a AWSCodeDeployRoleForLambda aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 28 de novembro de 2017, 14:05 UTC
- Horário editado: 03 de dezembro de 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "cloudwatch:DescribeAlarms",
    "lambda:UpdateAlias",
    "lambda:GetAlias",
    "lambda:GetProvisionedConcurrencyConfig",
    "sns:Publish"
  ],
  "Resource" : "*",
  "Effect" : "Allow"
},
{
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3::*/CodeDeploy/*",
  "Effect" : "Allow"
},
{
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectVersion"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
    }
  },
  "Effect" : "Allow"
},
{
  "Action" : [
    "lambda:InvokeFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
  "Effect" : "Allow"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeDeployRoleForLambdaLimited

`AWSCodeDeployRoleForLambdaLimited` é uma [política AWS gerenciada](#) que: Fornece acesso limitado ao serviço CodeDeploy para realizar uma implantação do Lambda em seu nome.

### A utilização desta política

Você pode vincular a `AWSCodeDeployRoleForLambdaLimited` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 17 de agosto de 2020, 17:14 UTC
- Horário editado: 17 de agosto de 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "cloudwatch:DescribeAlarms",
      "lambda:UpdateAlias",
      "lambda:GetAlias",
      "lambda:GetProvisionedConcurrencyConfig"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "arn:aws:s3::*:/CodeDeploy/*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
      }
    },
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda::*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodePipeline\_FullAccess

AWSCodePipeline\_FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total AWS CodePipeline por meio do AWS Management Console.

### Utilização desta política

Você pode vincular a `AWSCodePipeline_FullAccess` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 03 de agosto de 2020, 22:38 UTC
- Horário editado: 14 de março de 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "Statement" : [
    {
```

```
"Action" : [  
  "codepipeline:*",  
  "cloudformation:DescribeStacks",  
  "cloudformation:ListStacks",  
  "cloudformation:ListChangeSets",  
  "cloudtrail:DescribeTrails",  
  "codebuild:BatchGetProjects",  
  "codebuild:CreateProject",  
  "codebuild:ListCuratedEnvironmentImages",  
  "codebuild:ListProjects",  
  "codecommit:ListBranches",  
  "codecommit:GetReferences",  
  "codecommit:ListRepositories",  
  "codedeploy:BatchGetDeploymentGroups",  
  "codedeploy:ListApplications",  
  "codedeploy:ListDeploymentGroups",  
  "ec2:DescribeSecurityGroups",  
  "ec2:DescribeSubnets",  
  "ec2:DescribeVpcs",  
  "ecr:DescribeRepositories",  
  "ecr:ListImages",  
  "ecs:ListClusters",  
  "ecs:ListServices",  
  "elasticbeanstalk:DescribeApplications",  
  "elasticbeanstalk:DescribeEnvironments",  
  "iam:ListRoles",  
  "iam:GetRole",  
  "lambda:ListFunctions",  
  "events:ListRules",  
  "events:ListTargetsByRule",  
  "events:DescribeRule",  
  "opsworks:DescribeApps",  
  "opsworks:DescribeLayers",  
  "opsworks:DescribeStacks",  
  "s3:ListAllMyBuckets",  
  "sns:ListTopics",  
  "codestar-notifications:ListNotificationRules",  
  "codestar-notifications:ListTargets",  
  "codestar-notifications:ListTagsForResource",  
  "codestar-notifications:ListEventTypes",  
  "states:ListStateMachines"  
],  
"Effect" : "Allow",  
"Resource" : "*",
```

```
    "Sid" : "CodePipelineAuthoringAccess"
  },
  {
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:GetBucketPolicy",
      "s3:GetBucketVersioning",
      "s3:GetObjectVersion",
      "s3:CreateBucket",
      "s3:PutBucketPolicy"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:s3::*:codepipeline-*",
    "Sid" : "CodePipelineArtifactsReadWriteAccess"
  },
  {
    "Action" : [
      "cloudtrail:PutEventSelectors",
      "cloudtrail:CreateTrail",
      "cloudtrail:GetEventSelectors",
      "cloudtrail:StartLogging"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:cloudtrail::*:trail/codepipeline-source-trail",
    "Sid" : "CodePipelineSourceTrailReadWriteAccess"
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/cwe-role-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "EventsIAMPassRole"
  },
},
```

```
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "codepipeline.amazonaws.com"
      ]
    }
  },
  "Sid" : "CodePipelineIAMPassRole"
},
{
  "Action" : [
    "events:PutRule",
    "events:PutTargets",
    "events>DeleteRule",
    "events:DisableRule",
    "events:RemoveTargets"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:events:*:*:rule/codepipeline-*"
  ],
  "Sid" : "CodePipelineEventsReadWriteAccess"
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
```

```
    }
  }
},
{
  "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:SetTopicAttributes"
  ],
  "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
  "Action" : [
    "chatbot:DescribeSlackChannelConfigurations",
    "chatbot:ListMicrosoftTeamsChannelConfigurations"
  ],
  "Resource" : "*"
}
],
"Version" : "2012-10-17"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSCodePipeline\_ReadOnlyAccess

AWSCodePipeline\_ReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS CodePipeline por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSCodePipeline\_ReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de agosto de 2020, 22:25 UTC
- Horário editado: 03 de agosto de 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
```

```
    "s3:ListBucket",
    "s3:GetBucketPolicy"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:s3::*:codepipeline-*"
},
{
  "Sid" : "CodeStarNotificationsReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:DescribeNotificationRule"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
    }
  }
}
],
"Version" : "2012-10-17"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess é uma [política AWS gerenciada](#) que: fornece acesso para visualizar e aprovar alterações manuais em todos os pipelines

### A utilização desta política

Você pode vincular a AWSCodePipelineApproverAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de julho de 2016, 18:59 UTC
- Horário editado: 02 de agosto de 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess é uma [política AWS gerenciada](#) que: fornece acesso a ações personalizadas para pesquisar detalhes de trabalhos (incluindo credenciais temporárias) e relatar atualizações de status ao AWS CodePipeline.

### A utilização desta política

Você pode vincular a AWSCodePipelineCustomActionAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:02 UTC
- Horário editado: 09 de julho de 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
```

```
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
],
"Version" : "2012-10-17"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeStarFullAccess

`AWSCodeStarFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS CodeStar por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a `AWSCodeStarFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de abril de 2017, 16:23 UTC
- Horário editado: 28 de março de 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS CodeStar Notifications acesse o Amazon CloudWatch Events em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de novembro de 2019, 16:10 UTC
- Horário editado: 19 de março de 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "sns:CreateTopic"
    ],
    "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "codecommit:GetCommentsForPullRequest",
      "codecommit:GetCommentsForComparedCommit",
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:UpdateSlackChannelConfiguration",
      "codecommit:GetDifferences",
      "codepipeline:ListActionExecutions"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : [
      "codecommit:GetFile"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
      }
    },
    "Effect" : "Allow"
  }
]
```

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCodeStarServiceRole

AWSCodeStarServiceRole é uma [política AWS gerenciada](#) que: NÃO USE - AWS Política de função de serviço do CodeStar, que concede privilégios administrativos para que o CodeStar gerencie o IAM e outros recursos de serviço em nome do cliente.

## A utilização desta política

Você pode vincular a AWSCodeStarServiceRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de abril de 2017, 15:20 UTC
- Horário editado: 20 de setembro de 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

```
{
  "Sid" : "ProjectEventRules",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:RemoveTargets",
    "events:PutRule",
    "events>DeleteRule",
    "events:DescribeRule"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/awscodestar-*"
  ]
},
{
  "Sid" : "ProjectStack",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:*Stack*",
    "cloudformation:CreateChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation:GetTemplate"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awscodestar-*",
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
    "arn:aws:cloudformation:*:aws:transform/CodeStar*"
  ]
},
{
  "Sid" : "ProjectStackTemplate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "cloudformation:DescribeChangeSet"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectQuickstarts",
  "Effect" : "Allow",
  "Action" : [
```



```

    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::awscodestar-*/*"
  ]
},
{
  "Sid" : "ProjectS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:*"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-codestar-*",
    "arn:aws:s3:::elasticbeanstalk-*"
  ]
},
{
  "Sid" : "ProjectServices",
  "Effect" : "Allow",
  "Action" : [
    "codestar:*",
    "codecommit:*",
    "codepipeline:*",
    "codedeploy:*",
    "codebuild:*",
    "autoscaling:*",
    "cloudwatch:Put*",
    "ec2:*",
    "elasticbeanstalk:*",
    "elasticloadbalancing:*",
    "iam:ListRoles",
    "logs:*",
    "sns:*",
    "cloud9:CreateEnvironmentEC2",
    "cloud9>DeleteEnvironment",
    "cloud9:DescribeEnvironment*",
    "cloud9:ListEnvironments"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectWorkerRoles",
  "Effect" : "Allow",

```

```

    "Action" : [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:GetRole",
      "iam:PassRole",
      "iam:GetRolePolicy",
      "iam:PutRolePolicy",
      "iam:SetDefaultPolicyVersion",
      "iam:CreatePolicy",
      "iam>DeletePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam>CreateInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/CodeStarWorker*",
      "arn:aws:iam::*:policy/CodeStarWorker*",
      "arn:aws:iam::*:instance-profile/awscodestar-*"
    ]
  },
  {
    "Sid" : "ProjectTeamMembers",
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachUserPolicy",
      "iam:DetachUserPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyArn" : [
          "arn:aws:iam::*:policy/CodeStar_*"
        ]
      }
    }
  }
},
{
  "Sid" : "ProjectRoles",
  "Effect" : "Allow",
  "Action" : [

```

```
    "iam:CreatePolicy",
    "iam>DeletePolicy",
    "iam:CreatePolicyVersion",
    "iam>DeletePolicyVersion",
    "iam:ListEntitiesForPolicy",
    "iam:ListPolicyVersions",
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : [
    "arn:aws:iam::*:policy/CodeStar_*"
  ]
},
{
  "Sid" : "InspectServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-codestar-service-role",
    "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
  ]
},
{
  "Sid" : "IAMLinkRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "cloud9.amazonaws.com"
    }
  }
},
{
  "Sid" : "DescribeConfigRuleForARN",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConfigRules"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
  "Sid" : "ProjectCodeStarConnections",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codestar-connections:GetConnection"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ProjectCodeStarConnectionsPassConnections",
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine é uma [política AWS gerenciada](#) que: nega o acesso a determinadas ações, aplicada pela AWS equipe no caso de as credenciais de um usuário do IAM terem sido comprometidas ou expostas publicamente. NÃO remova essa política. Em vez disso, siga as instruções especificadas no e-mail enviado a você sobre este evento.

## A utilização desta política

Você pode vincular a `AWSCompromisedKeyQuarantine` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de agosto de 2020, 18:04 UTC
- Horário editado: 11 de agosto de 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",

```

```
    "iam:UpdateAccessKey",
    "iam:UpdateAccountPasswordPolicy",
    "iam:UpdateUser",
    "ec2:RequestSpotInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "organizations:CreateAccount",
    "organizations:CreateOrganization",
    "organizations:InviteAccountToOrganization",
    "lambda:CreateFunction",
    "lightsail:Create*",
    "lightsail:Start*",
    "lightsail>Delete*",
    "lightsail:Update*",
    "lightsail:GetInstanceAccessDetails",
    "lightsail:DownloadDefaultKeyPair"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2 é uma [política AWS gerenciada](#) que: nega o acesso a determinadas ações, aplicada pela AWS equipe no caso de as credenciais de um usuário do IAM terem sido comprometidas ou expostas publicamente. NÃO remova essa política. Em vez disso, siga as instruções especificadas no caso de suporte criado para você em relação a esse evento.

## A utilização desta política

Você pode vincular a `AWSCompromisedKeyQuarantineV2` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de abril de 2021, 22:30 UTC
- Horário editado: 16 de março de 2023, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
```

```
"iam:CreateRole",
"iam:CreateUser",
"iam:DetachUserPolicy",
"iam:PassRole",
"iam:PutGroupPolicy",
"iam:PutRolePolicy",
"iam:PutUserPermissionsBoundary",
"iam:PutUserPolicy",
"iam:SetDefaultPolicyVersion",
"iam:UpdateAccessKey",
"iam:UpdateAccountPasswordPolicy",
"iam:UpdateAssumeRolePolicy",
"iam:UpdateLoginProfile",
"iam:UpdateUser",
"lambda:AddLayerVersionPermission",
"lambda:AddPermission",
"lambda:CreateFunction",
"lambda:GetPolicy",
"lambda:ListTags",
"lambda:PutProvisionedConcurrencyConfig",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:UpdateFunctionCode",
"lightsail:Create*",
"lightsail:Delete*",
"lightsail:DownloadDefaultKeyPair",
"lightsail:GetInstanceAccessDetails",
"lightsail:Start*",
"lightsail:Update*",
"organizations:CreateAccount",
"organizations:CreateOrganization",
"organizations:InviteAccountToOrganization",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:PutLifecycleConfiguration",
"s3:PutBucketAcl",
"s3:PutBucketOwnershipControls",
"s3:DeleteBucketPolicy",
"s3:ObjectOwnerOverrideToBucketOwner",
"s3:PutAccountPublicAccessBlock",
"s3:PutBucketPolicy",
"s3:ListAllMyBuckets",
"ec2:PurchaseReservedInstancesOffering",
```



```
    "ec2:AcceptReservedInstancesExchangeQuote",
    "ec2:CreateReservedInstancesListing",
    "savingsplans:CreateSavingsPlan"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSConfigMultiAccountSetupPolicy

AWSConfigMultiAccountSetupPolicy é uma [política AWS gerenciada](#) que: permite que o Config chame AWS serviços e implante recursos de configuração em toda a organização

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora da criação: 17 de junho de 2019, 18:03 UTC
- Horário editado: 24 de fevereiro de 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config>DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
```

```

    "config:DeleteConformancePack"
  ],
  "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeConformancePackStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "config-conforms.amazonaws.com"
    }
  }
},
{
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Effect" : "Allow",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ssm.amazonaws.com"
    }
  }
}
]

```

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Config corrija recursos não compatíveis em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário da criação: 18 de junho de 2019, 21:21 UTC
- Horário editado: 18 de junho de 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ssm:GetDocument",
      "ssm:DescribeDocument",
      "ssm:StartAutomationExecution"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ssm.amazonaws.com"
      }
    },
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSConfigRoleForOrganizations

AWSConfigRoleForOrganizations é uma [política AWS gerenciada](#) que: Permite que o AWS Config chame APIs Organizations somente para leitura AWS

## A utilização desta política

Você pode vincular a AWSConfigRoleForOrganizations aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de março de 2018, 22:53 UTC
- Horário editado: 24 de novembro de 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCfgRulesExecutionRole

AWSCfgRulesExecutionRole é uma [política AWS gerenciada](#) que: Permite que uma função AWS Lambda acesse a API AWS Config e os snapshots de configuração que o Config AWS entrega periodicamente ao Amazon S3. Esse acesso é exigido por funções que avaliam as alterações de configuração das regras de Config personalizadas.

### A utilização desta política

Você pode vincular a AWSCfgRulesExecutionRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 25 de março de 2016, 17:59 UTC
- Horário editado: 13 de maio de 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCfgRulesExecutionRole`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:Put*",
      "config:Get*",
      "config:List*",
      "config:Describe*",
      "config:BatchGet*",
      "config:Select*"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSConfigServiceRolePolicy

AWSConfigServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Config chame AWS serviços e colete configurações de recursos em seu nome.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.



## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de maio de 2018, 23:31 UTC
- Horário editado: 22 de fevereiro de 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

## Versão da política

Versão da política: v50 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",

```

```
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:ListApps",
"amplify:ListBranches",
"amplifyuibuilder:ExportThemes",
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"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/*"
      ]
    }
  ]
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)



# AWSConfigUserAccess

`AWSConfigUserAccess` é uma [política gerenciada da AWS](#) que: fornece acesso para usar o AWS Config, incluindo pesquisa por tags em recursos e leitura de todas as tags. Isso não fornece permissão para configurar o AWS Config, o que requer privilégios administrativos.

## A utilização desta política

Você pode vincular a `AWSConfigUserAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de fevereiro de 2015, 19:38 UTC
- Horário editado: 18 de março de 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",

```

```
    "tag:GetResources",
    "tag:GetTagKeys",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:LookupEvents"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSConnector

AWSConnector é uma [política AWS gerenciada](#) que: permite amplo acesso de leitura/gravação a TODOS os objetos do EC2, acesso de leitura/gravação aos buckets do S3 começando com 'import-to-ec2' e a capacidade de listar todos os buckets do S3 para que o Connector importe VMs em seu nome. AWS

## Utilização desta política

Você pode vincular a AWSConnector aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 11 de fevereiro de 2015, 17:14 UTC
- Hora da edição: 28 de setembro de 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3>DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CancelConversionTask",
  "ec2:CancelExportTask",
  "ec2:CreateImage",
  "ec2:CreateInstanceExportTask",
  "ec2:CreateTags",
  "ec2:CreateVolume",
  "ec2>DeleteTags",
  "ec2>DeleteVolume",
  "ec2:DescribeConversionTasks",
  "ec2:DescribeExportTasks",
  "ec2:DescribeImages",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceStatus",
  "ec2:DescribeInstances",
  "ec2:DescribeRegions",
  "ec2:DescribeTags",
  "ec2:DetachVolume",
  "ec2:ImportInstance",
  "ec2:ImportVolume",
  "ec2:ModifyInstanceAttribute",
  "ec2:RunInstances",
  "ec2:StartInstances",
  "ec2:StopInstances",
  "ec2:TerminateInstances",
  "ec2:ImportImage",
  "ec2:DescribeImportImageTasks",
  "ec2:DeregisterImage",
  "ec2:DescribeSnapshots",
  "ec2>DeleteSnapshot",
  "ec2:CancelImportTask",
  "ec2:ImportSnapshot",
  "ec2:DescribeImportSnapshotTasks"
],
"Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSControlTowerAccountServiceRolePolicy

`AWSControlTowerAccountServiceRolePolicy` é uma [política AWS gerenciada](#) que: Permite que a AWS Control Tower ligue para AWS serviços que fornecem configuração automatizada de contas e governança centralizada em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de junho de 2023, 22:04 UTC
- Horário editado: 05 de junho de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events>DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
```

```
"Action" : [
  "events:DescribeRule",
  "events:ListTargetsByRule"
],
"Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
},
{
  "Sid" : "AllowControlTowerToPublishSecurityNotifications",
  "Effect" : "Allow",
  "Action" : "sns:publish",
  "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
},
{
  "Sid" : "AllowActionsForSecurityHubIntegration",
  "Effect" : "Allow",
  "Action" : [
    "securityhub:DescribeStandardsControls",
    "securityhub:GetEnabledStandards"
  ],
  "Resource" : "arn:aws:securityhub:*:*:hub/default"
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS recursos gerenciados ou usados pela AWS Control Tower

## A utilização desta política

Você pode vincular a `AWSControlTowerServiceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 03 de maio de 2019, 18:19 UTC
- Horário editado: 12 de abril de 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

## Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation>DeleteStack",
        "cloudformation>DeleteStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",

```



```

    "cloudformation:UpdateStackInstances",
    "cloudformation:UpdateStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CreateStackInstances",
    "cloudformation:CreateStackSet",
    "cloudformation>DeleteStack",
    "cloudformation>DeleteStackInstances",
    "cloudformation>DeleteStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:GetTemplate",
    "cloudformation>ListStackInstances",
    "cloudformation:UpdateStack",
    "cloudformation:UpdateStackInstances",
    "cloudformation:UpdateStackSet"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/**",
    "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
    "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/**"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateTrail",
    "cloudtrail>DeleteTrail",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:StartLogging",
    "cloudtrail:StopLogging",
    "cloudtrail:UpdateTrail",
    "cloudtrail:PutEventSelectors",
    "logs:CreateLogStream",

```

```

    "logs:PutLogEvents",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
    "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-controltower*/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sts:AssumeRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/AWSControlTowerExecution",
    "arn:aws:iam:*:*:role/AWSControlTowerBlueprintAccess"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:DescribeTrails",
    "ec2:DescribeAvailabilityZones",
    "iam:ListRoles",
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups",
    "organizations:CreateAccount",
    "organizations:DescribeAccount",
    "organizations:DescribeCreateAccountStatus",
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribePolicy",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListAWSServiceAccessForOrganization",

```

```

    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListParents",
    "organizations:ListPoliciesForTarget",
    "organizations:ListTargetsForPolicy",
    "organizations:ListRoots",
    "organizations:MoveAccount",
    "servicecatalog:AssociatePrincipalWithPortfolio"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListAttachedRolePolicies",
    "iam:GetRolePolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
    "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
    "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "config>DeleteConfigurationAggregator",
    "config:PutConfigurationAggregator",
    "config:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
    }
  }
}

```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "config.amazonaws.com",
        "cloudtrail.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "account:EnableRegion",
    "account:ListRegions",
    "account:GetRegionOptStatus"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicy é uma [política AWS gerenciada](#) que: concede permissões para descrever a organização da conta, criar buckets S3 para o programa MAP e aplicar tags a ele, criar um relatório de custo e uso e descrever as definições do relatório de custo e uso.

### A utilização desta política

Você pode vincular a AWSCostAndUsageReportAutomationPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de novembro de 2021, 21:27 UTC
- Horário editado: 01 de novembro de 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur>DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataExchangeFullAccess

`AWSDataExchangeFullAccess` é uma [política AWS gerenciada](#) que: Concede acesso total ao AWS Data Exchange e AWS Marketplace às ações usando o AWS Management Console e SDK. Ele também fornece acesso seletivo aos serviços relacionados necessários para aproveitar ao máximo o AWS Data Exchange.

### A utilização desta política

Você pode vincular a `AWSDataExchangeFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de novembro de 2019, 19:27 UTC
- Horário editado: 02 de dezembro de 2021, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:*"
    ],
    "Resource" : "*"
  },
  {
    "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: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"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe",
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:GetAgreementRequest",
      "aws-marketplace:ListAgreementRequests",
      "aws-marketplace:CancelAgreementRequest"
    ]
  }
}
```

```
    ],
    "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" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess` é uma [política AWS gerenciada](#) que: Concede ao provedor de dados acesso ao AWS Data Exchange e AWS Marketplace às ações usando o AWS Management Console e SDK. Ele também fornece acesso seletivo aos serviços relacionados necessários para aproveitar ao máximo o AWS Data Exchange.

### A utilização desta política

Você pode vincular a `AWSDataExchangeProviderFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de novembro de 2019, 19:27 UTC
- Horário editado: 15 de março de 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataExchangeReadOnly

AWSDataExchangeReadOnly é uma [política gerenciada da AWS](#) que: Concede acesso somente leitura ao AWS Data Exchange e às ações AWS Marketplace usando o AWS Management Console e o SDK.

## A utilização desta política

Você pode vincular a `AWSDataExchangeReadOnly` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de novembro de 2019, 19:27 UTC
- Horário editado: 10 de maio de 2021, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataExchangeSubscriberFullAccess

AWSDataExchangeSubscriberFullAccess é uma [política AWS gerenciada](#) que: Concede aos assinantes de dados acesso ao AWS Data Exchange e às AWS Marketplace ações usando o AWS Management Console e SDK. Ele também fornece acesso seletivo aos serviços relacionados necessários para aproveitar ao máximo o AWS Data Exchange.

### A utilização desta política

Você pode vincular a AWSDataExchangeSubscriberFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de novembro de 2019, 19:27 UTC
- Horário editado: 29 de novembro de 2021, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "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:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
```

```
    "kms:ListKeys"  
  ],  
  "Resource" : "*" ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole` é uma [política AWS gerenciada](#) que: Fornece permissões apropriadas ao AWS Data Lifecycle Manager para realizar ações sobre os recursos AWS

### A utilização desta política

Você pode vincular a `AWSDataLifecycleManagerServiceRole` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de julho de 2018, 19:34 UTC
- Horário editado: 19 de setembro de 2022, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier"
      ],
      "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.*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataLifecycleManagerServiceRoleForAMIManagement

AWSDataLifecycleManagerServiceRoleForAMIManagement é uma [política AWS gerenciada](#) que: Fornece permissões apropriadas ao AWS Data Lifecycle Manager para realizar ações sobre os AWS recursos para o gerenciamento de AMI

### A utilização desta política

Você pode vincular a AWSDataLifecycleManagerServiceRoleForAMIManagement aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 21 de outubro de 2020, 19:39 UTC
- Horário editado: 19 de agosto de 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2>DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
```

```
    "ec2:CopyImage",
    "ec2:ModifyImageAttribute"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:EnableImageDeprecation",
    "ec2:DisableImageDeprecation"
  ],
  "Resource" : "arn:aws:ec2:*::image/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDatalifecycleManagerSSMFullAccess

AWSDatalifecycleManagerSSMFullAccess é uma [política gerenciada pela AWS](#) que: fornece ao Amazon Data Lifecycle Manager permissão para realizar as ações do Systems Manager necessárias para executar scripts anteriores e posteriores em todas as instâncias do Amazon EC2.

### Utilização desta política

Você pode vincular a AWSDatalifecycleManagerSSMFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 31 de outubro de 2023, 20:29 UTC



- Horário editado: 16 de novembro de 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:DescribeDocument",
    "ssm:GetDocument"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
    "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
  ]
},
{
  "Sid" : "AllowAllEC2Instances",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSDataPipeline\_FullAccess

AWSDataPipeline\_FullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao Data Pipeline, acesso à lista para funções do S3, DynamoDB, Redshift, RDS, SNS e IAM e acesso ao PassRole para funções padrão.

## A utilização desta política

Você pode vincular a AWSDataPipeline\_FullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de janeiro de 2017, 23:14 UTC
- Horário editado: 17 de agosto de 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",

```

```
    "sns:Subscribe",
    "iam:ListRoles",
    "iam:GetRolePolicy",
    "iam:GetInstanceProfile",
    "iam:ListInstanceProfiles",
    "datapipeline:*"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
    "arn:aws:iam::*:role/DataPipelineDefaultRole"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDatapipeline\_PowerUser

AWSDatapipeline\_PowerUser é uma [política AWS gerenciada](#) que: fornece acesso total ao Data Pipeline, acesso à lista para funções do S3, DynamoDB, Redshift, RDS, SNS e IAM e acesso ao PassRole para funções padrão.

## A utilização desta política

Você pode vincular a AWSDatapipeline\_PowerUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de janeiro de 2017, 23:16 UTC
- Horário editado: 17 de agosto de 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```
{
  "Action" : "iam:PassRole",
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
    "arn:aws:iam::*:role/DataPipelineDefaultRole"
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataSyncDiscoveryServiceRolePolicy

AWSDataSyncDiscoveryServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o DataSync Discovery se integre a AWS outros serviços em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de março de 2023, 22:19 UTC
- Horário editado: 20 de março de 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
    }
  ]
}
```

```
    "Resource" : [
      "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDataSyncFullAccess

AWSDataSyncFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total AWS DataSync e acesso mínimo às suas dependências

### Utilização desta política

Você pode vincular a AWSDataSyncFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 18 de janeiro de 2019, 19:40 UTC
- Horário editado: 16 de fevereiro de 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.



## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSDataSyncReadOnlyAccess

AWSDataSyncReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao AWS DataSync.

### A utilização desta política

Você pode vincular a AWSDataSyncReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de janeiro de 2019, 19:18 UTC
- Horário editado: 30 de junho de 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDepLensLambdaFunctionAccessPolicy

AWSDepLensLambdaFunctionAccessPolicy é uma [política AWS gerenciada que: Essa política](#) especifica as permissões exigidas pelas funções lambda administrativas do DeepLens que são executadas em um dispositivo do DeepLens

### A utilização desta política

Você pode vincular a AWSDepLensLambdaFunctionAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 15:47 UTC
- Horário editado: 11 de junho de 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDepLensLambdaFunctionAccessPolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3objectAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::deeplens/*",
    "arn:aws:s3:::deeplens*"
  ]
},
{
  "Sid" : "DeepLensGreenGrassCloudWatchAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents",
    "logs:CreateLogGroup"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
},
{
  "Sid" : "DeepLensAccess",
  "Effect" : "Allow",
  "Action" : [
    "deeplens:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensKinesisVideoAccess",
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:DescribeStream",
    "kinesisvideo:CreateStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:PutMedia"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepLensServiceRolePolicy

AWSDeepLensServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede ao AWS DeepLens acesso, recursos e funções necessários Serviços da AWS para o DeepLens e suas dependências, incluindo IoT, S3, GreenGrass e Lambda. AWS

## A utilização desta política

Você pode vincular a AWSDeepLensServiceRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 29 de novembro de 2017, 15:46 UTC
- Horário editado: 25 de setembro de 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot>DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:AttachPrincipalPolicy"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:policy/deeplens*",
      "arn:aws:iot:*:*:cert/*"
    ]
  },
  {
    "Sid" : "DeepLensIoTDataAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:GetThingShadow",
      "iot:UpdateThingShadow"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:thing/deeplens*"
    ]
  },
  {
    "Sid" : "DeepLensIoTEndpointAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeEndpoint"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DeepLensAccess",
    "Effect" : "Allow",
    "Action" : [
      "deeplens:*"
    ],
    "Resource" : [
```



```
        "*"
    ]
},
{
    "Sid" : "DeepLensS3ObjectAccess",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::deeplens*"
    ]
},
{
    "Sid" : "DeepLensS3Buckets",
    "Effect" : "Allow",
    "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::deeplens*"
    ]
},
{
    "Sid" : "DeepLensCreateS3Buckets",
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "DeepLensIAMPassRoleAccess",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
```

```
    "StringEquals" : {
      "iam:PassedToService" : [
        "greengrass.amazonaws.com",
        "sagemaker.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "DeepLensIAMLambdaPassRoleAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/AWSDeepLens*",
      "arn:aws:iam::*:role/service-role/AWSDeepLens*"
    ],
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "DeepLensGreenGrassAccess",
    "Effect" : "Allow",
    "Action" : [
      "greengrass:AssociateRoleToGroup",
      "greengrass:AssociateServiceRoleToAccount",
      "greengrass:CreateResourceDefinition",
      "greengrass:CreateResourceDefinitionVersion",
      "greengrass:CreateCoreDefinition",
      "greengrass:CreateCoreDefinitionVersion",
      "greengrass:CreateDeployment",
      "greengrass:CreateFunctionDefinition",
      "greengrass:CreateFunctionDefinitionVersion",
      "greengrass:CreateGroup",
      "greengrass:CreateGroupCertificateAuthority",
      "greengrass:CreateGroupVersion",
      "greengrass:CreateLoggerDefinition",
      "greengrass:CreateLoggerDefinitionVersion",
      "greengrass:CreateSubscriptionDefinition",
      "greengrass:CreateSubscriptionDefinitionVersion",
```

```
"greengrass:DeleteCoreDefinition",
"greengrass:DeleteFunctionDefinition",
"greengrass:DeleteGroup",
"greengrass:DeleteLoggerDefinition",
"greengrass:DeleteSubscriptionDefinition",
"greengrass:DisassociateRoleFromGroup",
"greengrass:DisassociateServiceRoleFromAccount",
"greengrass:GetAssociatedRole",
"greengrass:GetConnectivityInfo",
"greengrass:GetCoreDefinition",
"greengrass:GetCoreDefinitionVersion",
"greengrass:GetDeploymentStatus",
"greengrass:GetDeviceDefinition",
"greengrass:GetDeviceDefinitionVersion",
"greengrass:GetFunctionDefinition",
"greengrass:GetFunctionDefinitionVersion",
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
"greengrass:ListGroups",
"greengrass:ListLoggerDefinitionVersions",
"greengrass:ListLoggerDefinitions",
"greengrass:ListSubscriptionDefinitionVersions",
"greengrass:ListSubscriptionDefinitions",
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
```

```
    "greengrass:UpdateFunctionDefinition",
    "greengrass:UpdateGroup",
    "greengrass:UpdateGroupCertificateConfiguration",
    "greengrass:UpdateLoggerDefinition",
    "greengrass:UpdateSubscriptionDefinition",
    "greengrass:UpdateResourceDefinition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DeepLensLambdaAdminFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda>ListFunctions",
    "lambda>ListVersionsByFunction",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:deeplens*"
  ]
},
{
  "Sid" : "DeepLensLambdaUsersFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda>ListFunctions",
    "lambda>ListVersionsByFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*"
  ]
},
{
  "Sid" : "DeepLensSageMakerWriteAccess",
```

```
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateTrainingJob",
      "sagemaker:DescribeTrainingJob",
      "sagemaker:StopTrainingJob"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:training-job/deeplens*"
    ]
  },
  {
    "Sid" : "DeepLensSageMakerReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribeTrainingJob"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:training-job/*"
    ]
  },
  {
    "Sid" : "DeepLensKinesisVideoStreamAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:CreateStream",
      "kinesisvideo:DescribeStream",
      "kinesisvideo>DeleteStream"
    ],
    "Resource" : [
      "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
    ]
  },
  {
    "Sid" : "DeepLensKinesisVideoEndpointAccess",
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:GetDataEndpoint"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess é uma [política AWS gerenciada](#) que: acesso administrativo do DeepRacer a todas as ações, incluindo alternar entre o modo multiusuário e o modo de usuário único.

## A utilização desta política

Você pode vincular a AWSDeepRacerAccountAdminAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de outubro de 2021, 01:27 UTC
- Horário editado: 28 de outubro de 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepRacerCloudFormationAccessPolicy

AWSDeepRacerCloudFormationAccessPolicy é uma [política AWS gerenciada](#) que: Permite que o CloudFormation crie e AWS gerencie pilhas e recursos em seu nome.

## A utilização desta política

Você pode vincular a `AWSDeepRacerCloudFormationAccessPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de fevereiro de 2019, 21:59 UTC
- Horário editado: 14 de junho de 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```



```
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateNetworkAcl",
    "ec2:CreateNetworkAclEntry",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:CreateVpcEndpoint",
    "ec2>DeleteInternetGateway",
    "ec2>DeleteNatGateway",
    "ec2>DeleteNetworkAcl",
    "ec2>DeleteNetworkAclEntry",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteSubnet",
    "ec2>DeleteTags",
    "ec2>DeleteVpc",
    "ec2>DeleteVpcEndpoints",
    "ec2:DescribeAddresses",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:DetachInternetGateway",
    "ec2:DisassociateRouteTable",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ReleaseAddress",
    "ec2:ReplaceNetworkAclAssociation",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
```

```

    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
    "Condition" : {
      "StringLikeIfExists" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:CreateFunction",
      "lambda:GetFunction",
      "lambda>DeleteFunction",
      "lambda:TagResource",
      "lambda:UpdateFunctionCode"
    ],
    "Resource" : [
      "arn:aws:lambda::*:function:*DeepRacer*",
      "arn:aws:lambda::*:function:*Deepracer*",
      "arn:aws:lambda::*:function:*deepracer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutBucketPolicy",
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3>DeleteBucket"
    ],
    "Resource" : [
      "arn:aws:s3::*:DeepRacer*",
      "arn:aws:s3::*:Deepracer*",
      "arn:aws:s3::*:deepracer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [

```

```
    "robomaker:CreateSimulationApplication",
    "robomaker:CreateSimulationApplicationVersion",
    "robomaker>DeleteSimulationApplication",
    "robomaker:DescribeSimulationApplication",
    "robomaker>ListSimulationApplications",
    "robomaker:TagResource",
    "robomaker:UpdateSimulationApplication"
  ],
  "Resource" : [
    "arn:aws:robomaker:*:*:/createSimulationApplication",
    "arn:aws:robomaker:*:*:simulation-application/deepracer*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess é uma [política AWS gerenciada](#) que: DeepRacer MultiUser Acesso de usuário padrão para usar o deepracer no modo multiusuário

### A utilização desta política

Você pode vincular a AWSDeepRacerDefaultMultiUserAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de outubro de 2021, 01:27 UTC

- Horário editado: 28 de outubro de 2021, 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer>Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer>Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
```

```
    "depracer:UserToken" : "false"
  },
  "Bool" : {
    "depracer:MultiUser" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "depracer:GetAccountConfig",
    "depracer:GetTrack",
    "depracer:ListTracks",
    "depracer:TestRewardFunction"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Deny",
  "Action" : [
    "depracer:Admin*"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSDeepRacerFullAccess

AWSDeepRacerFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS DeepRacer. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3).

## A utilização desta política

Você pode vincular a AWSDeepRacerFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de outubro de 2020, 22:03 UTC
- Horário editado: 05 de outubro de 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```

    "Action" : [
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetBucketPolicy",
      "s3:PutBucketPolicy",
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:GetObjectAcl",
      "s3:GetBucketLocation"
    ],
    "Resource" : [
      "arn:aws:s3::*DeepRacer*",
      "arn:aws:s3::*Deepracer*",
      "arn:aws:s3::*deepracer*",
      "arn:aws:s3:::dr-*",
      "arn:aws:s3::*DeepRacer*/**",
      "arn:aws:s3::*Deepracer*/**",
      "arn:aws:s3::*deepracer*/**",
      "arn:aws:s3:::dr-*/**"
    ]
  }
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicy é uma [política AWS gerenciada](#) que: Permite que o RoboMaker crie os recursos necessários e chame os AWS serviços em seu nome.

## A utilização desta política

Você pode vincular a `AWSDeepRacerRoboMakerAccessPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de fevereiro de 2019, 21:59 UTC
- Horário editado: 28 de fevereiro de 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
```



```

    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
    "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::*DeepRacer*",
    "arn:aws:s3::*Deepracer*",
    "arn:aws:s3::*deepracer*",
    "arn:aws:s3::*dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/DeepRacer" : "true"
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesisvideo:CreateStream",
      "kinesisvideo:DescribeStream",
      "kinesisvideo:GetDataEndpoint",
      "kinesisvideo:PutMedia",
      "kinesisvideo:TagStream"
    ],
    "Resource" : [
      "arn:aws:kinesisvideo:*:*:stream/dr-*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o DeepRacer crie os recursos necessários e AWS chame os serviços em seu nome.

### A utilização desta política

Você pode vincular a AWSDeepRacerServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 28 de fevereiro de 2019, 21:58 UTC

- Horário editado: 12 de junho de 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
```

```
    "cloudformation:DetectStackDrift",
    "cloudformation:DescribeStackDriftDetectionStatus",
    "cloudformation:DescribeStackResourceDrifts"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "robomaker.amazonaws.com"
    }
  },
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSDeepRacer*",
    "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
```

```

    "lambda:InvokeFunction",
    "lambda:UpdateFunctionCode"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*DeepRacer*",
    "arn:aws:lambda:*:*:function:*Deepracer*",
    "arn:aws:lambda:*:*:function:*deepracer*",
    "arn:aws:lambda:*:*:function:*dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutBucketPolicy",
    "s3:GetBucketAcl"
  ],
  "Resource" : [
    "arn:aws:s3::*:*DeepRacer*",
    "arn:aws:s3::*:*Deepracer*",
    "arn:aws:s3::*:*deepracer*",
    "arn:aws:s3::*:*dr-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/DeepRacer" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "kinesisvideo:CreateStream",

```

```
    "kinesisvideo:DeleteStream",
    "kinesisvideo:DescribeStream",
    "kinesisvideo:GetDataEndpoint",
    "kinesisvideo:GetHLSStreamingSessionURL",
    "kinesisvideo:GetMedia",
    "kinesisvideo:PutMedia",
    "kinesisvideo:TagStream"
  ],
  "Resource" : [
    "arn:aws:kinesisvideo:*:*:stream/dr-*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDenyAll

AWSDenyAll é uma [política gerenciada pela AWS](#) que: negue todo o acesso.

### Utilização desta política

Você pode vincular a AWSDenyAll aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 01 de maio de 2019, 22:36 UTC
- Horário editado: 18 de dezembro de 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDeviceFarmFullAccess

AWSDeviceFarmFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as operações AWS do Device Farm.

## A utilização desta política

Você pode vincular a `AWSDeviceFarmFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de julho de 2015, 16:37 UTC
- Horário editado: 13 de julho de 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDDeviceFarmServiceRolePolicy

AWSDDeviceFarmServiceRolePolicy é uma [política AWS gerenciada](#) que: Conceda permissões ao AWS Device Farm para chamar as APIs de rede do EC2 em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de setembro de 2022, 21:02 UTC
- Horário editado: 20 de setembro de 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDDeviceFarmServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
```

```
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/AWSDeviceFarmManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    }
  }
},
{
  "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateNetworkInterfacePermission",
  "ec2>DeleteNetworkInterface"
],
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy é uma [política AWS gerenciada](#) que: conceda permissões ao AWS Device Farm para chamar APIs do EC2 em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de maio de 2021, 22:01 UTC
- Horário editado: 26 de maio de 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/AWSDeviceFarmManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface"
    ],
  },
```

```
"Resource" : "arn:aws:ec2:*:*:network-interface/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Direct Connect por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a `AWSDirectConnectFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 30 de abril de 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDirectConnectReadOnlyAccess

`AWSDirectConnectReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS Direct Connect por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a `AWSDirectConnectReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 18 de maio de 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "directconnect:Describe*",
      "directconnect:List*",
      "ec2:DescribeVpnGateways",
      "ec2:DescribeTransitGateways"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDirectConnectServiceRolePolicy

AWSDirectConnectServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece permissão do AWS Direct Connect para criar e gerenciar AWS recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de janeiro de 2021, 18:35 UTC
- Horário editado: 14 de janeiro de 2021, 18:35 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSDirectoryServiceFullAccess

`AWSDirectoryServiceFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Directory Service.

## A utilização desta política

Você pode vincular a `AWSDirectoryServiceFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 24 de novembro de 2020, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
},
{
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Effect" : "Allow",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "ds.amazonaws.com"
    }
  }
},
},
```

```
{
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDirectoryServiceReadOnlyAccess

`AWSDirectoryServiceReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS Directory Service.

### A utilização desta política

Você pode vincular a `AWSDirectoryServiceReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 25 de setembro de 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDiscoveryContinuousExportFirehosePolicy

AWSDiscoveryContinuousExportFirehosePolicy é uma [política AWS gerenciada](#) que: Fornece acesso de gravação aos AWS recursos necessários para o AWS Discovery Continuous Export

### A utilização desta política

Você pode vincular a AWSDiscoveryContinuousExportFirehosePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de agosto de 2018, 18:29 UTC
- Horário editado: 08 de junho de 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "glue:GetTableVersions"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-application-discovery-service-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-stream:*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o DMS Fleet Advisor gerencie as métricas do CloudWatch em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 06 de março de 2023, 09:10 UTC
- Horário editado: 06 de março de 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

```
}  
}  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSDMSServerlessServiceRolePolicy

AWSDMSServerlessServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede permissões sem servidor ao AWS DMS para criar e gerenciar recursos do DMS em sua conta em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de maio de 2023, 20:28 UTC
- Horário editado: 18 de maio de 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms>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:*"
  ]
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy é uma [política AWS gerenciada](#) que: Permite que o serviço EC2 CapacityReservation Fleet gerencie reservas de capacidade

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de setembro de 2021, 14:43 UTC
- Horário editado: 29 de setembro de 2021, 14:43 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "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"
      }
    }
  }
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy é uma [política AWS gerenciada](#) que: permite que o EC2 Fleet lance e gerencie instâncias.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de março de 2018, 00:08 UTC
- Horário editado: 04 de maio de 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:spot-instances-request/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
```



```
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEC2SpotFleetServiceRolePolicy

AWSEC2SpotFleetServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o EC2 Spot Fleet lance e gereencie instâncias da frota spot

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de outubro de 2017, 19:13 UTC
- Horário editado: 16 de março de 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ],
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:spot-instances-request/*",
      "arn:aws:ec2:*:*:spot-fleet-request/*",
      "arn:aws:ec2:*:*:volume*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:loadbalancer*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:*/*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o EC2 Spot lance e gere instâncias spot

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de setembro de 2017, 18:51 UTC
- Horário editado: 12 de dezembro de 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Action" : [
  "ec2:DescribeInstances",
  "ec2:StartInstances",
  "ec2:StopInstances",
  "ec2:RunInstances"
],
"Resource" : [
  "*"
]
},
{
  "Effect" : "Deny",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "ec2:InstanceMarketType" : "spot"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSECRPullThroughCache\_ServiceRolePolicy

AWSECRPullThroughCache\_ServiceRolePolicy é uma [política gerenciada pela AWS](#) que: permite o acesso aos serviços e recursos da AWS usados ou gerenciados pelo cache pull through da AWS ECR.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2021, 21:51 UTC
- Hora da edição: 13 de novembro de 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkCustomPlatformforEC2Role

AWSElasticBeanstalkCustomPlatformforEC2Role é uma [política AWS gerenciada](#) que: forneça à instância em seu ambiente personalizado de criação de plataformas permissão para iniciar a instância EC2, criar um snapshot e AMI do EBS, transmitir logs para o Amazon CloudWatch Logs e armazenar artefatos no Amazon S3.

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkCustomPlatformforEC2Role aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de fevereiro de 2017, 22:50 UTC
- Horário editado: 21 de fevereiro de 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Statement" : [
  {
    "Sid" : "EC2Access",
    "Action" : [
      "ec2:AttachVolume",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CopyImage",
      "ec2:CreateImage",
      "ec2:CreateKeypair",
      "ec2:CreateSecurityGroup",
      "ec2:CreateSnapshot",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2>DeleteKeypair",
      "ec2>DeleteSecurityGroup",
      "ec2>DeleteSnapshot",
      "ec2>DeleteVolume",
      "ec2:DeregisterImage",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeRegions",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeTags",
      "ec2:DescribeVolumes",
      "ec2:DetachVolume",
      "ec2:GetPasswordData",
      "ec2:ModifyImageAttribute",
      "ec2:ModifyInstanceAttribute",
      "ec2:ModifySnapshotAttribute",
      "ec2:RegisterImage",
      "ec2:RunInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "BucketAccess",
    "Action" : [
      "s3:Get*",

```

```

    "s3:List*",
    "s3:PutObject"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkEnhancedHealth

AWSElasticBeanstalkEnhancedHealth é uma [política AWS gerenciada que: Política](#) do AWS Elastic Beanstalk Service para o sistema de monitoramento de saúde

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkEnhancedHealth aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 08 de fevereiro de 2016, 23:17 UTC
- Horário editado: 09 de abril de 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkMaintenance

AWSElasticBeanstalkMaintenance é uma [política AWS gerenciada que: AWS Política](#) de função de serviço do Elastic Beanstalk que concede permissões limitadas para atualizar seus recursos em seu nome para fins de manutenção.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 11 de janeiro de 2019, 23:22 UTC
- Horário editado: 04 de junho de 2019, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy é uma [política AWS gerenciada](#) que: [Essa política](#) é para a função de serviço do AWS Elastic Beanstalk usada para realizar atualizações gerenciadas dos ambientes do Elastic Beanstalk. Essa política não deve ser vinculada a outros usuários ou funções. A política concede amplas permissões para criar e gerenciar recursos em vários AWS serviços, incluindo AutoScaling, EC2, ECS, Elastic Load Balancing e CloudFormation. Essa política também permite a transmissão de qualquer função do IAM utilizável com esses serviços.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de março de 2021, 22:18 UTC
- Horário editado: 23 de março de 2023, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
```

```
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLoadBalancers",
    "autoscaling:DescribeNotificationConfigurations",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeScheduledActions",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "logs:DescribeLogGroups",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2BroadOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion",
```



```

    "ec2:CreateSecurityGroup",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions",
    "ec2>DeleteSecurityGroup",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2RunInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "EC2TerminateInstancesOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  }
},
{
  "Sid" : "ECSBroadOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:DescribeClusters",

```

```

    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ECSDeleteClusterOperationPermissions",
  "Effect" : "Allow",
  "Action" : "ecs:DeleteCluster",
  "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
},
{
  "Sid" : "ASGOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteScheduledAction",
    "autoscaling:DetachInstances",
    "autoscaling>DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:ResumeProcesses",
    "autoscaling:SetDesiredCapacity",
    "autoscaling:SuspendProcesses",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
},
{
  "Sid" : "CFNOperationPermissions",
  "Effect" : "Allow",
  "Action" : [

```

```

    "cloudformation:*"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "ELB0perationPermissions",
  "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" : "CWLogs0perationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
  "Sid" : "S30bject0perationPermissions",
  "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"
          ]
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy é uma [política AWS gerenciada](#) que: [AWS Política](#) de função de serviço do Elastic Beanstalk que concede permissões limitadas para atualizações gerenciadas.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de novembro de 2019, 22:35 UTC
- Horário editado: 24 de março de 2023, 00:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
```

```
        "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
        ]
    }
}
},
{
    "Sid" : "SingleInstanceAPIs",
    "Effect" : "Allow",
    "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ECS",
    "Effect" : "Allow",
    "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ElasticBeanstalkAPIs",
    "Effect" : "Allow",
    "Action" : [
        "elasticbeanstalk:*"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ReadOnlyAPIs",
    "Effect" : "Allow",
```

```

    "Action" : [
      "cloudformation:Describe*",
      "cloudformation:List*",
      "ec2:Describe*",
      "autoscaling:Describe*",
      "elasticloadbalancing:Describe*",
      "logs:DescribeLogGroups",
      "sns:GetTopicAttributes",
      "sns:ListSubscriptionsByTopic",
      "rds:DescribeDBEngineVersions",
      "rds:DescribeDBInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ASG",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DetachInstances",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:ResumeProcesses",
      "autoscaling:SuspendProcesses",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup"
    ],
    "Resource" : [
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
    ]
  },
  {
    "Sid" : "CFN",

```



```

    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation:CancelUpdateStack",
      "cloudformation>DeleteStack",
      "cloudformation:GetTemplate",
      "cloudformation:UpdateStack"
    ],
    "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"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDocker é uma [política AWS gerenciada](#) que: Forneça às instâncias em seu ambiente Docker de vários contêineres acesso para usar o Amazon EC2 Container Service para gerenciar tarefas de implantação de contêineres.

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkMulticontainerDocker aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de fevereiro de 2016, 23:15 UTC
- Horário editado: 23 de março de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Sid" : "ECSAccess",
"Effect" : "Allow",
"Action" : [
  "ecs:Poll",
  "ecs:StartTask",
  "ecs:StopTask",
  "ecs:DiscoverPollEndpoint",
  "ecs:StartTelemetrySession",
  "ecs:RegisterContainerInstance",
  "ecs:DeregisterContainerInstance",
  "ecs:DescribeContainerInstances",
  "ecs:Submit*",
  "ecs:DescribeTasks"
],
"Resource" : "*"
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "RegisterContainerInstance",
        "StartTask"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly é uma [política AWS gerenciada](#) que: Concede permissões somente para leitura. Permite explicitamente que os operadores obtenham acesso direto para recuperar informações sobre recursos relacionados aos aplicativos do Elastic AWS Beanstalk.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de janeiro de 2021, 19:02 UTC
- Horário editado: 22 de janeiro de 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
```

```
"autoscaling:DescribeLoadBalancers",
"autoscaling:DescribeNotificationConfigurations",
"autoscaling:DescribeScalingActivities",
"autoscaling:DescribeScheduledActions",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"cloudformation:GetTemplate",
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ValidateTemplate",
"cloudtrail:LookupEvents",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplateVersions",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSSLPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"iam:GetRole",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListRolePolicies",
```

```
    "iam:ListRoles",
    "iam:ListServerCertificates",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribeDBSnapshots",
    "s3:ListAllMyBuckets",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowS3",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore é uma [política AWS gerenciada](#) que:

AWSElasticBeanstalkRoleCore (função de operações do Elastic Beanstalk) Permite a operação principal de um ambiente de serviço web.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkRoleCore aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:48 UTC
- Horário editado: 09 de setembro de 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/awseb-e-*"
    }
}
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReleaseAddress",
    "ec2:AllocateAddress",
    "ec2:DisassociateAddress",
    "ec2:AssociateAddress",
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteSecurityGroup",
    "ec2:AuthorizeSecurityGroup*",
    "ec2:RevokeSecurityGroup*",
    "ec2:CreateLaunchTemplate*",
    "ec2>DeleteLaunchTemplate*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LTRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:*LoadBalancer*",
    "autoscaling:*AutoScalingGroup",
    "autoscaling:*LaunchConfiguration",
    "autoscaling>DeleteScheduledAction",
```

```

        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
    ],
    "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
    ]
},
{
    "Sid" : "ASGPolicy",
    "Effect" : "Allow",
    "Action" : [
        "autoscaling:DeletePolicy"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "EBSLR",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
    ],
    "Condition" : {
        "StringLike" : {
            "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
    }
},
{
    "Sid" : "S30bj",
    "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"
    ],
    "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"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkRoleCWL

AWSElasticBeanstalkRoleCWL é uma [política AWS gerenciada](#) que: (função de operações do Elastic Beanstalk) Permite que um ambiente gerencie grupos de log do Amazon CloudWatch Logs.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkRoleCWL aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:49 UTC
- Horário editado: 05 de junho de 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS é uma [política AWS gerenciada](#) que: (função de operações do Elastic Beanstalk) permite que um ambiente Docker de vários contêineres gerencie clusters do Amazon ECS.

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkRoleECS aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:47 UTC
- Horário editado: 23 de março de 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "ecs:CreateCluster",
    "ecs>DeleteCluster",
    "ecs:RegisterTaskDefinition",
    "ecs:DeRegisterTaskDefinition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "CreateCluster",
        "RegisterTaskDefinition"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkRoleRDS

AWSElasticBeanstalkRoleRDS é uma [política AWS gerenciada](#) que: (função de operações do Elastic Beanstalk) permite que um ambiente integre uma instância do Amazon RDS.

## A utilização desta política

Você pode vincular a `AWSElasticBeanstalkRoleRDS` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:46 UTC
- Horário editado: 05 de junho de 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds>DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds>CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds>DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS é uma [política AWS gerenciada](#) que: (função de operações do Elastic Beanstalk) permite que um ambiente habilite a integração de tópicos do Amazon SNS.

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkRoleSNS aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:46 UTC
- Horário editado: 05 de junho de 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns>DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticBeanstalkRoleWorkerTier

AWSElasticBeanstalkRoleWorkerTier é uma [política AWS gerenciada](#) que: (função de operações do Elastic Beanstalk) permite que um nível de ambiente de operador crie uma tabela do Amazon DynamoDB e uma fila do Amazon SQS.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkRoleWorkerTier aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2020, 21:43 UTC
- Horário editado: 05 de junho de 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
```

```
    "sqs:DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:CreateQueue"
  ],
  "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
},
{
  "Sid" : "AllowDDB",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb:TagResource",
    "dynamodb:DescribeTable",
    "dynamodb>DeleteTable"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkService

AWSElasticBeanstalkService é uma [política gerenciada da AWS](#) que: Essa política está em um caminho de suspensão de uso. Consulte a documentação para obter orientação: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Política de função do Elastic Beanstalk Service que concede permissões para criar e gerenciar recursos (ou seja: AutoScaling, EC2, S3, CloudFormation, ELB etc.) em seu nome.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkService aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de abril de 2016, 20:27 UTC
- Horário editado: 10 de maio de 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

## Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    }
  ]
}
```

```
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "CreateCluster",
        "RegisterTaskDefinition"
      ]
    }
  }
},
{
  "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:*"
  ],
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "AllowLaunchTemplateRunInstances",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
    }
  }
},
{
  "Sid" : "AllowELBAddTags",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags"
  ]
}
```



```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "elasticloadbalancing:CreateAction" : [
          "CreateLoadBalancer"
        ]
      }
    }
  },
  {
    "Sid" : "AllowOperations",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling:CreateOrUpdateTags",
      "autoscaling>DeleteLaunchConfiguration",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling>DeleteScheduledAction",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeLaunchConfigurations",
      "autoscaling:DescribeLoadBalancers",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:DescribeScalingActivities",
      "autoscaling:DescribeScheduledActions",
      "autoscaling:DetachInstances",
      "autoscaling>DeletePolicy",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:ResumeProcesses",
      "autoscaling:SetDesiredCapacity",
      "autoscaling:SuspendProcesses",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup",
      "cloudwatch:PutMetricAlarm",
      "ec2:AssociateAddress",
      "ec2:AllocateAddress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
```

```
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeLaunchTemplateVersions",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2:CreateSecurityGroup",
"ec2>DeleteSecurityGroup",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeVpcClassicLink",
"ec2:DisassociateAddress",
"ec2:ReleaseAddress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:TerminateInstances",
"ecs:CreateCluster",
"ecs>DeleteCluster",
"ecs:DescribeClusters",
"ecs:RegisterTaskDefinition",
"elasticbeanstalk:*",
"elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
"elasticloadbalancing:ConfigureHealthCheck",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing>DeleteLoadBalancer",
"elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:RegisterInstancesWithLoadBalancer",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:DeregisterTargets",
"iam:ListRoles",
"iam:PassRole",
```

```
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy",
    "logs:DescribeLogGroups",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:ListBucket",
    "sns:CreateTopic",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "sns:Subscribe",
    "sns:SetTopicAttributes",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticBeanstalkServiceRolePolicy

AWSElasticBeanstalkServiceRolePolicy é uma [política AWS gerenciada que: política](#) do AWS Elastic Beanstalk Service Linked Role que concede permissões para criar e gerenciar recursos (ou seja, AutoScaling, EC2, S3, CloudFormation, ELB etc.) em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de setembro de 2017, 23:46 UTC
- Horário editado: 06 de junho de 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/awseb-*",
      "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
  },
  {
    "Sid" : "AllowOperations",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:DescribeScalingActivities",
      "autoscaling:PutNotificationConfiguration",
      "ec2:DescribeInstanceStatus",
      "ec2:AssociateAddress",
      "ec2:DescribeAddresses",
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "elasticloadbalancing:DescribeInstanceHealth",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeTargetGroups",
      "lambda:GetFunction",
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl",
      "sns:Publish"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowOperationsOnHealthStreamingLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs>DeleteLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
```

```
}  
]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier é uma [política AWS gerenciada](#) que: Forneça às instâncias em seu ambiente de servidor web acesso para fazer upload de arquivos de log para o Amazon S3.

### A utilização desta política

Você pode vincular a AWSElasticBeanstalkWebTier aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de fevereiro de 2016, 23:08 UTC
- Horário editado: 09 de setembro de 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "BucketAccess",
    "Action" : [
      "s3:Get*",
      "s3:List*",
      "s3:PutObject"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:s3:::elasticbeanstalk-*",
      "arn:aws:s3:::elasticbeanstalk-*/*"
    ]
  },
  {
    "Sid" : "XRayAccess",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingRules",
      "xray:GetSamplingTargets",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchLogsAccess",
    "Action" : [
      "logs:PutLogEvents",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
    ]
  },
  {
    "Sid" : "ElasticBeanstalkHealthAccess",
    "Action" : [
      "elasticbeanstalk:PutInstanceStatistics"
    ],
  },
```

```
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:elasticbeanstalk:*:*:application/*",
      "arn:aws:elasticbeanstalk:*:*:environment/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTier é uma [política AWS gerenciada](#) que: forneça às instâncias em seu ambiente de trabalho acesso para carregar arquivos de log para o Amazon S3, usar o Amazon SQS para monitorar a fila de trabalhos do seu aplicativo, usar o Amazon DynamoDB para realizar a eleição do líder e para o Amazon CloudWatch publicar métricas para monitoramento de saúde.

## A utilização desta política

Você pode vincular a AWSElasticBeanstalkWorkerTier aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de fevereiro de 2016, 23:12 UTC
- Horário editado: 09 de setembro de 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`



## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
},
{
  "Sid" : "BucketAccess",
  "Action" : [
    "s3:Get*",
    "s3:List*",
    "s3:PutObject"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:s3:::elasticbeanstalk-*",
    "arn:aws:s3:::elasticbeanstalk-*/*"
  ]
},
{
  "Sid" : "DynamoPeriodicTasks",
  "Action" : [
    "dynamodb:BatchGetItem",
    "dynamodb:BatchWriteItem",
    "dynamodb:DeleteItem",
    "dynamodb:GetItem",
    "dynamodb:PutItem",
    "dynamodb:Query",
    "dynamodb:Scan",
    "dynamodb:UpdateItem"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
  ]
},
{
  "Sid" : "CloudWatchLogsAccess",
  "Action" : [
    "logs:PutLogEvents",
    "logs:CreateLogStream"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
  ]
},
{
  "Sid" : "ElasticBeanstalkHealthAccess",
```

```
    "Action" : [
      "elasticbeanstalk:PutInstanceStatistics"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:elasticbeanstalk:*:*:application/*",
      "arn:aws:elasticbeanstalk:*:*:environment/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryAgentInstallationPolicy

AWSElasticDisasterRecoveryAgentInstallationPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite instalar o Agente de AWS Replicação, que é usado com o AWS Elastic Disaster Recovery (DRS) para recuperar servidores externos em. AWS Anexe essa política aos usuários ou funções do IAM cujas credenciais você fornece durante a etapa de instalação do AWS Replication Agent.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryAgentInstallationPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 17 de novembro de 2021, 10:37 UTC

- Horário editado: 27 de novembro de 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticDisasterRecoveryAgentPolicy

AWSElasticDisasterRecoveryAgentPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite usar o Agente de AWS Replicação, que é usado com o AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem em. AWS Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

## Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryAgentPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 17 de novembro de 2021, 10:32 UTC
- Horário editado: 27 de novembro de 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
```

```

    "drs:UpdateAgentSourcePropertiesForDrs",
    "drs:UpdateAgentReplicationInfoForDrs",
    "drs:UpdateAgentConversionInfoForDrs",
    "drs:GetAgentCommandForDrs",
    "drs:GetAgentConfirmedResumeInfoForDrs",
    "drs:GetAgentRuntimeConfigurationForDrs",
    "drs:UpdateAgentBacklogForDrs",
    "drs:GetAgentReplicationInfoForDrs",
    "drs:IssueAgentCertificateForDrs"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
},
{
  "Sid" : "DRSAgentPolicy2",
  "Effect" : "Allow",
  "Action" : [
    "drs:GetAgentInstallationAssetsForDrs"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryConsoleFullAccess

AWSElasticDisasterRecoveryConsoleFullAccess é uma [política AWS gerenciada que: Essa política](#) fornece acesso total a todas as APIs públicas do AWS Elastic Disaster Recovery (DRS), bem como permissões para ler a chave KMS, o License Manager, os Resource Groups, o Elastic Load Balancing, o IAM e as informações do EC2. Anexe essa política aos seus usuários ou funções do IAM.

## A utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryConsoleFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de novembro de 2021, 10:46 UTC
- Horário editado: 16 de outubro de 2023, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
    }
  ]
}
```



```
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstanceTypeOfferings",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeVolumes",
      "ec2:GetEbsEncryptionByDefault",
      "ec2:GetEbsDefaultKmsKeyId",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeHosts"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess4",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess5",
    "Effect" : "Allow",
    "Action" : "resource-groups: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"
    ],
    "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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryConsoleFullAccess\_v2

AWSElasticDisasterRecoveryConsoleFullAccess\_v2 é uma [política AWS gerenciada](#) que: Essa política fornece acesso total a todas as APIs públicas do AWS Elastic Disaster Recovery (AWSDRS), bem como a todas as APIs públicas em outros AWS serviços usados pelo AWS DRS Console. Anexe essa política aos seus usuários ou funções.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryConsoleFullAccess\_v2 aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 27 de novembro de 2023, 13:35 UTC
- Horário editado: 27 de novembro de 2023, 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
```

```
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeHosts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess4",
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess5",
  "Effect" : "Allow",
  "Action" : "resource-groups:ListGroups",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess6",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess7",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListInstanceProfiles",
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess8",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
```

```

    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
      "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"
    ],
    "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"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticDisasterRecoveryConversionServerPolicy

`AWSElasticDisasterRecoveryConversionServerPolicy` é uma [política gerenciada pela AWS](#) que: Essa política é anexada à função de instância do servidor AWS Elastic Disaster Recovery Conversion. Essa política permite que os servidores de conversão do Elastic Disaster Recovery (DRS), que são instâncias EC2 lançadas pelo Elastic Disaster Recovery, se comuniquem com o serviço DRS. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pelo DRS aos servidores de conversão do DRS, que são iniciados e encerrados automaticamente pelo DRS, quando necessário. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM. Os servidores de conversão DRS são usados pelo Elastic Disaster Recovery quando os usuários optam por recuperar servidores de origem usando o console, a CLI ou a API do DRS.

## Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryConversionServerPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 17 de novembro de 2021, 13:42 UTC
- Horário editado: 27 de novembro de 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "DRSConversionServerPolicy1",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendClientMetricsForDrs",
      "drs:SendClientLogsForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSConversionServerPolicy2",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetChannelCommandsForDrs",
      "drs:SendChannelCommandResultForDrs"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite que o AWS Elastic Disaster Recovery (DRS) ofereça suporte à replicação entre contas e ao failback entre contas.

## Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 14 de maio de 2023, 07:16 UTC
- Horário editado: 17 de janeiro de 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryEc2InstancePolicy

AWSElasticDisasterRecoveryEc2InstancePolicy é uma [política gerenciada pela AWS](#) que: Essa política permite instalar e usar o Agente de AWS Replicação, que é usado pelo AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem executados no EC2 (entre regiões ou entre AZ). Uma função do IAM com essa política deve ser anexada (como um perfil de instância do EC2) às instâncias do EC2.

## Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryEc2InstancePolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de maio de 2022, 12:30 UTC
- Horário editado: 27 de novembro de 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
    }
  ]
}
```

```

    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceServerForDrs"
      }
    }
  },
  {
    "Sid" : "DRSEc2InstancePolicy3",
    "Effect" : "Allow",
    "Action" : [
      "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-network/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceNetwork"
      }
    }
  },
  {
    "Sid" : "DRSEc2InstancePolicy4",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendAgentMetricsForDrs",
      "drs:SendAgentLogsForDrs",
      "drs:UpdateAgentSourcePropertiesForDrs",
      "drs:UpdateAgentReplicationInfoForDrs",
      "drs:UpdateAgentConversionInfoForDrs",
      "drs:GetAgentCommandForDrs",
      "drs:GetAgentConfirmedResumeInfoForDrs",
      "drs:GetAgentRuntimeConfigurationForDrs",
      "drs:UpdateAgentBacklogForDrs",
      "drs:GetAgentReplicationInfoForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*"
  },
  {
    "Sid" : "DRSEc2InstancePolicy5",
    "Effect" : "Allow",
    "Action" : [
      "sts:AssumeRole",
      "sts:TagSession"
    ],
    "Resource" : [

```

```
    "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
    },
    "ForAnyValue:StringEquals" : {
      "sts:TransitiveTagKeys" : "SourceInstanceARN"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryFailbackInstallationPolicy

AWSElasticDisasterRecoveryFailbackInstallationPolicy é uma [política AWS gerenciada](#) que: Você pode anexar a AWSElasticDisasterRecoveryFailbackInstallationPolicy política às suas identidades do IAM. Essa política permite instalar o Elastic Disaster Recovery Failback Client, que é usado para retornar instâncias de recuperação à sua infraestrutura de origem. Anexe essa política aos seus usuários ou perfis do IAM cujas credenciais você fornece ao executar o Elastic Disaster Recovery Failback Client.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryFailbackInstallationPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 17 de novembro de 2021, 11:02 UTC
- Horário editado: 27 de novembro de 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",

```

```
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryFailbackPolicy

AWSElasticDisasterRecoveryFailbackPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite usar o Elastic Disaster Recovery Failback Client, que é usado para retornar instâncias de recuperação à sua infraestrutura de origem original. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

## Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryFailbackPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 17 de novembro de 2021, 10:41 UTC
- Horário editado: 27 de novembro de 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
```

```
"Action" : [
  "drs:GetFailbackCommandForDrs",
  "drs:UpdateFailbackClientLastSeenForDrs",
  "drs:NotifyAgentAuthenticationForDrs",
  "drs:UpdateAgentReplicationProcessStateForDrs",
  "drs:NotifyAgentReplicationProgressForDrs",
  "drs:NotifyAgentConnectedForDrs",
  "drs:NotifyAgentDisconnectedForDrs",
  "drs:NotifyConsistencyAttainedForDrs",
  "drs:GetFailbackLaunchRequestedForDrs",
  "drs:IssueAgentCertificateForDrs"
],
"Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryLaunchActionsPolicy

AWSElasticDisasterRecoveryLaunchActionsPolicy é uma [política AWS gerenciada](#) que: Essa política permite que você use o Amazon SSM e os serviços adicionais necessários para executar ações de pós-lançamento no AWS Elastic Disaster Recovery (AWSDRS). Anexe essa política às suas funções ou usuários do IAM.

### A utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryLaunchActionsPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 13 de setembro de 2023, 07:38 UTC
- Horário editado: 16 de outubro de 2023, 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "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"  
    }  
  }  
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryNetworkReplicationPolicy

AWSElasticDisasterRecoveryNetworkReplicationPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite que o AWS Elastic Disaster Recovery (DRS) ofereça suporte à replicação de rede.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryNetworkReplicationPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 11 de junho de 2023, 12:36 UTC

- Horário editado: 02 de janeiro de 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryReadOnlyAccess

AWSElasticDisasterRecoveryReadOnlyAccess é uma [política AWS gerenciada](#) que: Você pode anexar a AWSElasticDisasterRecoveryReadOnlyAccess política às suas identidades do IAM. Essa política fornece permissões para todas as APIs públicas somente para leitura do Elastic Disaster Recovery (DRS), bem como algumas APIs somente para leitura de outros AWS serviços que são necessárias para fazer uso total do console do DRS em somente leitura. Anexe essa política aos seus usuários ou funções do IAM.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 17 de novembro de 2021, 10:50 UTC
- Horário editado: 27 de novembro de 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "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"
      }
    }
  }

```

```
    }  
  }  
} ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryRecoveryInstancePolicy

AWSElasticDisasterRecoveryRecoveryInstancePolicy é uma [política gerenciada pela AWS](#) que: Essa política está vinculada à função de instância da Instância de Recuperação do Elastic Disaster Recovery. Essa política permite que a Instância de Recuperação do Elastic Disaster Recovery (DRS), que são instâncias do EC2 lançadas pela Elastic Disaster Recovery, se comunique com o serviço DRS e seja capaz de dar failback à sua infraestrutura de origem. Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela Elastic Disaster Recovery às instâncias de recuperação do DRS. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryRecoveryInstancePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 17 de novembro de 2021, 10:20 UTC
- Horário editado: 27 de novembro de 2023, 13:11 UTC

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

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
```

```
    "Effect" : "Allow",
    "Action" : [
      "drs:DescribeRecoveryInstances"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceTypes"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy4",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetAgentInstallationAssetsForDrs",
      "drs:SendClientLogsForDrs",
      "drs:CreateSourceServerForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy5",
    "Effect" : "Allow",
    "Action" : [
      "drs:TagResource"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*",
    "Condition" : {
      "StringEquals" : {
        "drs:CreateAction" : "CreateSourceServerForDrs"
      }
    }
  },
  {
    "Sid" : "DRSRecoveryInstancePolicy6",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendAgentMetricsForDrs",
      "drs:SendAgentLogsForDrs",
      "drs:UpdateAgentSourcePropertiesForDrs",
```



```

        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
    ],
    "Resource" : "arn:aws:drs:*:*:source-server/*"
},
{
    "Sid" : "DRSRecoveryInstancePolicy7",
    "Effect" : "Allow",
    "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
    ],
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
            "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
    }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElasticDisasterRecoveryReplicationServerPolicy

`AWSElasticDisasterRecoveryReplicationServerPolicy` é uma [política gerenciada pela AWS](#) que: Essa política é anexada à função de instância do servidor Elastic Disaster Recovery Replication. Essa política permite que os servidores de replicação do Elastic Disaster Recovery (DRS), que são instâncias EC2 lançadas pelo Elastic Disaster Recovery, se comuniquem com o serviço DRS e criem snapshots do EBS no seu. Conta da AWS Uma função do IAM com essa política é anexada (como um perfil de instância do EC2) pela Elastic Disaster Recovery aos servidores de replicação do DRS, que são automaticamente iniciados e encerrados pelo DRS, conforme necessário. Os servidores de replicação DRS são usados para facilitar a replicação de dados de seus servidores externos para AWS, como parte do processo de recuperação gerenciado pelo DRS. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

## Utilização desta política

Você pode vincular a `AWSElasticDisasterRecoveryReplicationServerPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 17 de novembro de 2021, 13:34 UTC
- Horário editado: 27 de novembro de 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "DRSReplicationServerPolicy1",
    "Effect" : "Allow",
    "Action" : [
      "drs:SendClientMetricsForDrs",
      "drs:SendClientLogsForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy2",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetChannelCommandsForDrs",
      "drs:SendChannelCommandResultForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy3",
    "Effect" : "Allow",
    "Action" : [
      "drs:GetAgentSnapshotCreditsForDrs",
      "drs:DescribeReplicationServerAssociationsForDrs",
      "drs:DescribeSnapshotRequestsForDrs",
      "drs:BatchDeleteSnapshotRequestForDrs",
      "drs:NotifyAgentAuthenticationForDrs",
      "drs:BatchCreateVolumeSnapshotGroupForDrs",
      "drs:UpdateAgentReplicationProcessStateForDrs",
      "drs:NotifyAgentReplicationProgressForDrs",
      "drs:NotifyAgentConnectedForDrs",
      "drs:NotifyAgentDisconnectedForDrs",
      "drs:NotifyVolumeEventForDrs",
      "drs:SendVolumeStatsForDrs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy4",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots"
    ]
  }
]
```

```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DRSReplicationServerPolicy5",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSReplicationServerPolicy6",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSReplicationServerPolicy7",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSnapshot"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryServiceRolePolicy

AWSElasticDisasterRecoveryServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Essa política permite que o Elastic Disaster Recovery gerencie AWS recursos em seu nome.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de novembro de 2021, 10:56 UTC
- Horário editado: 17 de janeiro de 2024, 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    }
  ]
}
```

```
"Sid" : "DRSServiceRolePolicy6",
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeImages",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceTypes",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceState",
  "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" : "*"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy é uma [política gerenciada pela AWS](#) que: Essa política permite acesso somente de leitura aos recursos do AWS Elastic Disaster Recovery (DRS), como servidores de origem e trabalhos. Também permite criar um instantâneo convertido e compartilhar esse instantâneo do EBS com uma conta específica.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryStagingAccountPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço

- Horário de criação: 26 de maio de 2022, 09:49 UTC
- Horário editado: 27 de novembro de 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

```
    },
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticDisasterRecoveryStagingAccountPolicy\_v2

AWSElasticDisasterRecoveryStagingAccountPolicy\_v2 é uma [política gerenciada pela AWS](#) que: Essa política é usada pelo AWS Elastic Disaster Recovery (DRS) para recuperar servidores de origem em uma conta de destino separada e permitir falhas. Não recomendamos que você anexe essa política aos seus usuários ou funções do IAM.

### Utilização desta política

Você pode vincular a AWSElasticDisasterRecoveryStagingAccountPolicy\_v2 aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 05 de janeiro de 2023, 12:11 UTC
- Horário editado: 27 de novembro de 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ],
  {
```

```
    "Sid" : "DRSStagingAccountPolicyv23",
    "Effect" : "Allow",
    "Action" : "drs:IssueAgentCertificateForDrs",
    "Resource" : [
      "arn:aws:drs:*:*:source-server/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticLoadBalancingClassicServiceRolePolicy

AWSElasticLoadBalancingClassicServiceRolePolicy é uma [política AWS gerenciada](#) que: Service Linked Role Policy for AWS Elastic Load Balancing Control Plane - Classic

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de setembro de 2017, 22:36 UTC
- Horário editado: 07 de outubro de 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElasticLoadBalancingServiceRolePolicy

AWSElasticLoadBalancingServiceRolePolicy é uma [política AWS gerenciada](#) que: Service Linked Role Policy for AWS Elastic Load Balancing Control Plane

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de setembro de 2017, 22:19 UTC
- Horário editado: 26 de agosto de 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeAddresses",
  "ec2:DescribeCoipPools",
  "ec2:DescribeInstances",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeSubnets",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeVpcs",
  "ec2:DescribeInternetGateways",
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeClassicLinkInstances",
  "ec2:DescribeVpcClassicLink",
  "ec2:CreateSecurityGroup",
  "ec2:CreateNetworkInterface",
  "ec2>DeleteNetworkInterface",
  "ec2:GetCoipPoolUsage",
  "ec2: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" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaConvertFullAccess

AWSElementalMediaConvertFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Elemental MediaConvert por meio do SDK e. AWS Management Console

### A utilização desta política

Você pode vincular a AWSElementalMediaConvertFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de junho de 2018, 19:25 UTC
- Horário editado: 10 de junho de 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "mediaconvert:*",
      "s3:ListAllMyBuckets",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "mediaconvert.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaConvertReadOnly

AWSElementalMediaConvertReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS Elemental MediaConvert por meio do SDK e. AWS Management Console

### A utilização desta política

Você pode vincular a AWSElementalMediaConvertReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de junho de 2018, 19:25 UTC
- Horário editado: 10 de junho de 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaLiveFullAccess

AWSElementalMediaLiveFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do AWS Elemental MediaLive

### A utilização desta política

Você pode vincular a AWSElementalMediaLiveFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de julho de 2020, 17:07 UTC
- Horário editado: 08 de julho de 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaLiveReadOnly

AWSElementalMediaLiveReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do AWS Elemental MediaLive

### A utilização desta política

Você pode vincular a AWSElementalMediaLiveReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de julho de 2020, 16:38 UTC
- Horário editado: 08 de julho de 2020, 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "medialive:List*",
  "medialive:Describe*"
],
"Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaPackageFullAccess

AWSElementalMediaPackageFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do AWS Elemental MediaPackage

### A utilização desta política

Você pode vincular a AWSElementalMediaPackageFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de dezembro de 2017, 23:39 UTC
- Horário editado: 29 de dezembro de 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaPackageReadOnly

AWSElementalMediaPackageReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do AWS Elemental MediaPackage

## A utilização desta política

Você pode vincular a AWSElementalMediaPackageReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de dezembro de 2017, 00:04 UTC
- Horário editado: 30 de dezembro de 2017, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaPackageV2FullAccess

AWSElementalMediaPackageV2FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do AWS Elemental MediaPackageV2.

## A utilização desta política

Você pode vincular a AWSElementalMediaPackageV2FullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de julho de 2023, 20:29 UTC
- Horário editado: 25 de julho de 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElementalMediaPackageV2ReadOnly

AWSElementalMediaPackageV2ReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do AWS Elemental MediaPackageV2.

## A utilização desta política

Você pode vincular a AWSElementalMediaPackageV2ReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de julho de 2023, 20:31 UTC
- Horário editado: 25 de julho de 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaStoreFullAccess

AWSElementalMediaStoreFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso completo de leitura e gravação a todas as APIs do MediaStore

### A utilização desta política

Você pode vincular a AWSElementalMediaStoreFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de março de 2018, 23:15 UTC
- Horário editado: 05 de março de 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Statement" : [
  {
    "Action" : [
      "mediastore:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaStoreReadOnly

AWSElementalMediaStoreReadOnly é uma [política AWS gerenciada](#) que: Fornece permissões somente de leitura para as APIs do MediaStore

### A utilização desta política

Você pode vincular a AWSElementalMediaStoreReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de março de 2018, 19:48 UTC
- Horário editado: 08 de março de 2018, 19:48 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSElementalMediaTailorFullAccess

AWSElementalMediaTailorFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos recursos do AWS Elemental MediaTailor

## A utilização desta política

Você pode vincular a AWSElementalMediaTailorFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de novembro de 2021, 00:04 UTC
- Horário editado: 23 de novembro de 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSElementalMediaTailorReadOnly

AWSElementalMediaTailorReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do AWS Elemental MediaTailor

### A utilização desta política

Você pode vincular a AWSElementalMediaTailorReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de novembro de 2021, 00:05 UTC
- Horário editado: 23 de novembro de 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

```
    "mediatailor:Describe*",
    "mediatailor:Get*"
  ],
  "Resource" : "*"
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEnhancedClassicNetworkingMangementPolicy

AWSEnhancedClassicNetworkingMangementPolicy é uma [política AWS gerenciada](#) que: Política para habilitar o recurso clássico aprimorado de gerenciamento de rede.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de setembro de 2017, 17:29 UTC
- Horário editado: 20 de setembro de 2017, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEntityResolutionConsoleFullAccess

AWSEntityResolutionConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao console à Resolução de AWS Entidades e aos serviços relacionados.

## A utilização desta política

Você pode vincular a AWSEntityResolutionConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 17 de agosto de 2023, 17:54 UTC
- Horário editado: 16 de outubro de 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "S3BucketsConsoleDisplay",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "S3SourcesConsoleDisplay",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:ListBucketVersions",
      "s3:GetBucketVersioning"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TaggingConsoleDisplay",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetTagKeys",
      "tag:GetTagValues"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KMSConsoleDisplay",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListRolesToPickRoleForPassing",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListRoles"
    ]
  }
}
```



```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PassRoleToEntityResolutionService",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "arn:aws:iam::*:role/*entityresolution*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "entityresolution.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ManageEventBridgeRules",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:PutTargets",
      "events:PutRule"
    ],
    "Resource" : [
      "arn:aws:events::*:rule/entity-resolution-automatic*"
    ]
  },
  {
    "Sid" : "ADXReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "dataexchange:GetDataSet"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura à Resolução de AWS Entidades por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a AWSEntityResolutionConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de agosto de 2023, 18:18 UTC
- Horário editado: 17 de agosto de 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFaultInjectionSimulatorEC2Access

AWSFaultInjectionSimulatorEC2Access é uma [política gerenciada pela AWS](#) que: Essa política concede ao Fault Injection Simulator Service permissão no EC2 e em outros serviços necessários para realizar ações do FIS.

### Utilização desta política

Você pode vincular a AWSFaultInjectionSimulatorEC2Access aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 20:39 UTC
- Horário editado: 27 de novembro de 2023, 15:08 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      },
      "Bool" : {
```

```
        "kms:GrantIsForAWSResource" : "true"
    }
}
},
{
    "Sid" : "AllowSSMSendOnEc2",
    "Effect" : "Allow",
    "Action" : [
        "ssm:SendCommand"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
    ]
},
{
    "Sid" : "AllowSSMStopOnEc2",
    "Effect" : "Allow",
    "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DescribeInstances",
    "Effect" : "Allow",
    "Action" : "ec2:DescribeInstances",
    "Resource" : "*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSFaultInjectionSimulatorECSAccess

AWSFaultInjectionSimulatorECSAccess é uma [política gerenciada pela AWS](#): Essa política concede ao Fault Injection Simulator Service permissão no ECS e em outros serviços necessários para realizar ações do FIS.

## Utilização desta política

Você pode vincular a AWSFaultInjectionSimulatorECSAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 20:37 UTC
- Horário editado: 25 de janeiro de 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:ListContainerInstances"
      ]
    }
  ],
}
```

```
    "Resource" : [
      "arn:aws:ecs:*:*:cluster/*"
    ]
  },
  {
    "Sid" : "Tasks",
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeTasks",
      "ecs:StopTask"
    ],
    "Resource" : [
      "arn:aws:ecs:*:*:task/*/*"
    ]
  },
  {
    "Sid" : "ContainerInstances",
    "Effect" : "Allow",
    "Action" : [
      "ecs:UpdateContainerInstancesState"
    ],
    "Resource" : [
      "arn:aws:ecs:*:*:container-instance/*/*"
    ]
  },
  {
    "Sid" : "ListTasks",
    "Effect" : "Allow",
    "Action" : [
      "ecs:ListTasks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SSMSend",
    "Effect" : "Allow",
    "Action" : "ssm:SendCommand",
    "Resource" : [
      "arn:aws:ssm:*:*:managed-instance/*",
      "arn:aws:ssm:*:*:document/*"
    ]
  },
  {
    "Sid" : "SSMList",
```

```
    "Effect" : "Allow",
    "Action" : [
      "ssm:ListCommands",
      "ssm:CancelCommand"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TargetResolutionByTags",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFaultInjectionSimulatorEKSAccess

AWSFaultInjectionSimulatorEKSAccess é uma [política gerenciada pela AWS](#): Essa política concede ao Fault Injection Simulator Service permissão no EKS e em outros serviços necessários para realizar ações do FIS.

### Utilização desta política

Você pode vincular a AWSFaultInjectionSimulatorEKSAccess aos seus usuários, grupos e perfis.



## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 20:34 UTC
- Hora da edição: 13 de novembro de 2023, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
```

```
    "Sid" : "DescribeCluster",
    "Effect" : "Allow",
    "Action" : "eks:DescribeCluster",
    "Resource" : "arn:aws:eks:*:*:cluster/*"
  },
  {
    "Sid" : "DescribeNodeGroup",
    "Effect" : "Allow",
    "Action" : "eks:DescribeNodegroup",
    "Resource" : "arn:aws:eks:*:*:nodegroup/*"
  },
  {
    "Sid" : "TargetResolutionByTags",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFaultInjectionSimulatorNetworkAccess

AWSFaultInjectionSimulatorNetworkAccess é uma [política gerenciada pela AWS](#): Essa política concede ao Fault Injection Simulator Service permissão na rede EC2 e em outros serviços necessários para realizar ações do FIS.

## Utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorNetworkAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 20:32 UTC
- Horário editado: 25 de janeiro de 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
```

```

    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkAcl",
    "Resource" : "arn:aws:ec2:*:*:network-acl/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteNetworkAcl",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkAclEntry",
      "ec2>DeleteNetworkAcl"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-acl/*",
      "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateNetworkAclOnVpc",
    "Effect" : "Allow",
    "Action" : "ec2:CreateNetworkAcl",
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "VpcActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs",
      "ec2:DescribeManagedPrefixLists",
      "ec2:DescribeSubnets",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcPeeringConnections",
      "ec2:DescribeRouteTables",

```

```

    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGateways"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReplaceNetworkAclAssociation",
  "Effect" : "Allow",
  "Action" : "ec2:ReplaceNetworkAclAssociation",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-acl/*"
  ]
},
{
  "Sid" : "GetManagedPrefixListEntries",
  "Effect" : "Allow",
  "Action" : "ec2:GetManagedPrefixListEntries",
  "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
},
{
  "Sid" : "CreateRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:CreateRouteTable",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateRouteTableOnVpc",
  "Effect" : "Allow",
  "Action" : "ec2:CreateRouteTable",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "CreateTagsOnRouteTable",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {

```

```
    "StringEquals" : {
      "ec2:CreateAction" : "CreateRouteTable",
      "aws:RequestTag/managedByFIS" : "true"
    }
  },
  {
    "Sid" : "CreateTagsOnNetworkInterface",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface",
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "CreateTagsOnPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateManagedPrefixList",
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteRouteTable",
    "Resource" : [
      "arn:aws:ec2:*:*:route-table/*",
      "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
},
```

```
{
  "Sid" : "CreateRoute",
  "Effect" : "Allow",
  "Action" : "ec2:CreateRoute",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterface",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterfaceOnSubnet",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group*"
  ]
},
{
  "Sid" : "DeleteNetworkInterface",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteNetworkInterface",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/managedByFIS" : "true"
    }
  }
},
{
  "Sid" : "CreateManagedPrefixList",
```

```

    "Effect" : "Allow",
    "Action" : "ec2:CreateManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DeleteManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ModifyManagedPrefixList",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyManagedPrefixList",
    "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ReplaceRouteTableAssociation",
    "Effect" : "Allow",
    "Action" : "ec2:ReplaceRouteTableAssociation",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*"
    ]
  },
  {
    "Sid" : "AssociateRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:AssociateRouteTable",

```



```

    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:route-table/*"
    ]
  },
  {
    "Sid" : "DisassociateRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:DisassociateRouteTable",
    "Resource" : [
      "arn:aws:ec2:*:*:route-table/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "DisassociateRouteTableOnSubnet",
    "Effect" : "Allow",
    "Action" : "ec2:DisassociateRouteTable",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*"
    ]
  },
  {
    "Sid" : "ModifyVpcEndpointOnRouteTable",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:route-table/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/managedByFIS" : "true"
      }
    }
  },
  {
    "Sid" : "ModifyVpcEndpoint",
    "Effect" : "Allow",
    "Action" : "ec2:ModifyVpcEndpoint",
    "Resource" : [

```

```
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
},
{
  "Sid" : "TransitGatewayRouteTableAssociation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateTransitGatewayRouteTable",
    "ec2:AssociateTransitGatewayRouteTable"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:transit-gateway-route-table/*",
    "arn:aws:ec2:*:*:transit-gateway-attachment/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess é uma [política gerenciada pela AWS](#): Essa política concede ao Fault Injection Simulator Service permissão no RDS e em outros serviços necessários para realizar ações do FIS.

### Utilização desta política

Você pode vincular a AWSFaultInjectionSimulatorRDSAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 20:30 UTC
- Hora da edição: 13 de novembro de 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    }
  ]
}
```

```
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess é uma [política AWS gerenciada](#) que: Essa política concede ao Fault Injection Simulator Service permissão no SSM e em outros serviços necessários para realizar ações do FIS.

## A utilização desta política

Você pode vincular a `AWSFaultInjectionSimulatorSSMAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 26 de outubro de 2022, 15:33 UTC
- Horário editado: 02 de junho de 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*: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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicy é uma [política AWS gerenciada](#) que: Política para permitir o acesso AWS service (Serviço da AWS) e os recursos usados ou gerenciados pela Amazon FinSpace

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de maio de 2023, 16:42 UTC
- Horário editado: 01 de dezembro de 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
```

```
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/FinSpace",
        "AWS/Usage"
      ]
    },
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFMAdminFullAccess

AWSFMAdminFullAccess é uma [política AWS gerenciada](#) que: Acesso total para AWS FM Administrator

### A utilização desta política

Você pode vincular a AWSFMAdminFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2018, 18:06 UTC
- Horário editado: 20 de outubro de 2022, 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

### Versão da política

Versão da política: v2 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "fms.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "fms.amazonaws.com"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess é uma [política AWS gerenciada](#) que: Acesso somente de leitura para o administrador de AWS FM que permite monitorar as operações de AWS FM

### A utilização desta política

Você pode vincular a AWSFMAdminReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2018, 20:07 UTC
- Horário editado: 31 de outubro de 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

```

    "waf:Get*",
    "waf:List*",
    "waf-regional:Get*",
    "waf-regional:List*",
    "firehose:ListDeliveryStreams",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "organizations:ListRoots",
    "organizations:ListChildren",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListOrganizationalUnitsForParent",
    "shield:GetSubscriptionState",
    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListAvailableManagedRuleGroups",
    "wafv2:CheckCapacity",
    "wafv2:ListAvailableManagedRuleGroupVersions",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:DescribeRuleGroupMetadata",
    "network-firewall:ListRuleGroups",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeRegions"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {

```

```
    "organizations:ServicePrincipal" : [  
      "fms.amazonaws.com"  
    ]  
  }  
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura às ações do AWS WAF para contas de membros AWS do Firewall Manager

### A utilização desta política

Você pode vincular a `AWSFMMemberReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2018, 21:05 UTC
- Horário editado: 09 de maio de 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSForWordPressPluginPolicy

AWSForWordPressPluginPolicy é uma [política AWS gerenciada que: Política gerenciada AWS](#) para o plug-in For Wordpress

## A utilização desta política

Você pode vincular a `AWSForWordPressPluginPolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de outubro de 2019, 00:27 UTC
- Horário editado: 20 de janeiro de 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",

```

```
    "s3:GetBucketPolicy",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:CreateBucket",
    "s3:PutObjectAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::audio_for_wordpress*",
    "arn:aws:s3:::audio-for-wordpress*"
  ]
},
{
  "Sid" : "Permissions3",
  "Effect" : "Allow",
  "Action" : [
    "acm:AddTagsToCertificate",
    "acm:DescribeCertificate",
    "acm:RequestCertificate",
    "cloudformation:CreateStack",
    "cloudfront:ListDistributions"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{
  "Sid" : "Permissions4",
  "Effect" : "Allow",
  "Action" : [
    "acm:DeleteCertificate",
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:UpdateStack",
    "cloudfront:CreateDistribution",
    "cloudfront:CreateInvalidation",
    "cloudfront:DeleteDistribution",
    "cloudfront:GetDistribution",
    "cloudfront:GetInvalidation",
    "cloudfront:TagResource",
    "cloudfront:UpdateDistribution"
  ]
}
```



```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGitSyncServiceRolePolicy

AWSGitSyncServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Política que permite que o AWS Code Connections sincronize conteúdo do seu repositório git

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de novembro de 2023, 17:05 UTC
- Hora da edição: 16 de novembro de 2023, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlobalAcceleratorSLRPolicy

AWSGlobalAcceleratorSLRPolicy é uma [política AWS gerenciada que: Política](#) que concede permissões ao AWS Global Accelerator para gerenciar interfaces de rede elástica e grupos de segurança do EC2.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de abril de 2019, 19:39 UTC
- Horário editado: 12 de setembro de 2023, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ]
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "EC2Action2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSecurityGroup",
      "ec2:AssignIpv6Addresses",
      "ec2:UnassignIpv6Addresses"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
      }
    }
  },
  {
    "Sid" : "EC2Action3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroups"
    ],
    "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/*"
    ]
  }
]
```

```
}  
]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlueConsoleFullAccess

AWSGlueConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Glue por meio do AWS Management Console

### A utilização desta política

Você pode vincular a AWSGlueConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de agosto de 2017, 13:37 UTC
- Horário editado: 14 de julho de 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "BaseAppPermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:*",
      "redshift:DescribeClusters",
      "redshift:DescribeClusterSubnetGroups",
      "iam:ListRoles",
      "iam:ListUsers",
      "iam:ListGroups",
      "iam:ListRolePolicies",
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListAttachedRolePolicies",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "rds:DescribeDBInstances",
      "rds:DescribeDBClusters",
      "rds:DescribeDBSubnetGroups",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3:GetBucketLocation",
      "cloudformation:ListStacks",
      "cloudformation:DescribeStacks",
      "cloudformation:GetTemplateSummary",
      "dynamodb:ListTables",
      "kms:ListAliases",
      "kms:DescribeKey",
      "cloudwatch:GetMetricData",
      "cloudwatch:ListDashboards",
      "databrew:ListRecipes",
      "databrew:ListRecipeVersions",
      "databrew:DescribeRecipe"
    ],
    "Resource" : [
```

```
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*/**",
        "arn:aws:s3:::*/*aws-glue-*/**",
        "arn:aws:s3:::aws-glue-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "tag:GetResources"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "logs:GetLogEvents"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
    ]
},
{
    "Effect" : "Allow",
```

```

    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:key-pair/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:volume*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
      },
      "StringEquals" : {
        "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ]
  }

```



```
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlueConsoleSageMakerNotebookFullAccess

`AWSGlueConsoleSageMakerNotebookFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Glue por meio de instâncias do notebook sagemaker AWS Management Console e acesso às instâncias do notebook sagemaker.

### A utilização desta política

Você pode vincular a `AWSGlueConsoleSageMakerNotebookFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de outubro de 2018, 17:52 UTC
- Horário editado: 15 de julho de 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "glue:*",
      "redshift:DescribeClusters",
      "redshift:DescribeClusterSubnetGroups",
      "iam:ListRoles",
      "iam:ListRolePolicies",
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListAttachedRolePolicies",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:CreateNetworkInterface",
      "ec2:AttachNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeNetworkInterfaces",
      "rds:DescribeDBInstances",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3:GetBucketLocation",
      "cloudformation:DescribeStacks",
      "cloudformation:GetTemplateSummary",
      "dynamodb:ListTables",
      "kms:ListAliases",
      "kms:DescribeKey",
      "sagemaker:ListNotebookInstances",
      "cloudformation:ListStacks",
      "cloudwatch:GetMetricData",
      "cloudwatch:ListDashboards"
    ],
  },
],
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*/*aws-glue-*/*",
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:/aws-glue/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue/*/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```

```

    "sagemaker:CreatePresignedNotebookInstanceUrl",
    "sagemaker:CreateNotebookInstance",
    "sagemaker>DeleteNotebookInstance",
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:StartNotebookInstance",
    "sagemaker:StopNotebookInstance",
    "sagemaker:UpdateNotebookInstance",
    "sagemaker:ListTags"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribeNotebookInstanceLifecycleConfig",
    "sagemaker:CreateNotebookInstanceLifecycleConfig",
    "sagemaker>DeleteNotebookInstanceLifecycleConfig",
    "sagemaker:ListNotebookInstanceLifecycleConfigs"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:volume*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
},

```

```

    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
      },
      "StringEquals" : {
        "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "aws:TagKeys" : [
          "aws-glue-*"
        ]
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam:*:*:role/AWSGlueServiceRole*",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  },
  {

```

```
"Action" : [
  "iam:PassRole"
],
"Effect" : "Allow",
"Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
"Condition" : {
  "StringLike" : {
    "iam:PassedToService" : [
      "ec2.amazonaws.com"
    ]
  }
}
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Action" : [
    "iam:PassRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com"
      ]
    }
  }
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AwsGlueDataBrewFullAccessPolicy

`AwsGlueDataBrewFullAccessPolicy` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Glue DataBrew por meio do. AWS Management Console Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, KMS, Glue).

## A utilização desta política

Você pode vincular a `AwsGlueDataBrewFullAccessPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de novembro de 2020, 16:51 UTC
- Horário editado: 04 de fevereiro de 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew>DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew>DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew>DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
        "databrew>DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",

```

```
    "databrew:DeleteSchedule",
    "databrew:CreateRuleset",
    "databrew:DeleteRuleset",
    "databrew:DescribeRuleset",
    "databrew:ListRulesets",
    "databrew:UpdateRuleset",
    "databrew:ListTagsForResource",
    "databrew:TagResource",
    "databrew:UntagResource"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "appflow:DescribeFlow",
    "appflow:DescribeFlowExecutionRecords",
    "appflow:ListFlows",
    "glue:GetConnection",
    "glue:GetConnections",
    "glue:GetDatabases",
    "glue:GetPartitions",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetDataCatalogEncryptionSettings",
    "dataexchange:ListDataSets",
    "dataexchange:ListDataSetRevisions",
    "dataexchange:ListRevisionAssets",
    "dataexchange:CreateJob",
    "dataexchange:StartJob",
    "dataexchange:GetJob",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "kms:DescribeKey",
    "kms:ListKeys",
    "kms:ListAliases",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSubnetGroups",
    "redshift-data:DescribeStatement",
    "redshift-data:ListDatabases",
    "redshift-data:ListSchemas",
```

```

    "redshift-data:ListTables",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "sts:GetCallerIdentity",
    "cloudtrail:LookupEvents",
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateConnection"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabases"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateTable"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",

```

```

    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::databrew-public-datasets-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateDataKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "kms:GenerateRandom"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",

```

```
"Action" : [
  "secretsmanager:GetSecretValue"
],
"Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "databrew.amazonaws.com"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
  "Condition" : {
    "StringLike" : {
      "secretsmanager:Name" : "databrew!default"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "databrew.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam:*:*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "databrew.amazonaws.com"
      ]
    }
  }
}
]
```

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlueDataBrewServiceRole

`AWSGlueDataBrewServiceRole` é uma [política gerenciada pela AWS](#): Essa política concede permissão ao Glue para executar ações no catálogo de dados do Glue do usuário. Essa política também fornece permissão para ações do EC2 para permitir que o Glue crie ENI para se conectar a recursos no VPC, além de permitir que o Glue acesse dados registrados no lakeformation e permissão para acessar o cloudwatch do usuário.

### Utilização desta política

Você pode vincular a `AWSGlueDataBrewServiceRole` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 04 de dezembro de 2020, 21:26 UTC
- Horário editado: 20 de março de 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeVpcEndpoints",
  "ec2:DescribeRouteTables",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeVpcAttribute",
  "ec2:CreateNetworkInterface"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteNetworkInterface",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/aws-glue-service-resource" : "*"
    }
  },
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2GlueTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  },
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
```



```
    ]
  },
  {
    "Sid" : "GlueDatabrewLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
    ]
  },
  {
    "Sid" : "LakeFormationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataAccess"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "SecretsManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AWSGlueSchemaRegistryFullAccess

AWSGlueSchemaRegistryFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Glue Schema Registry Service

## A utilização desta política

Você pode vincular a AWSGlueSchemaRegistryFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de novembro de 2020, 00:19 UTC
- Horário editado: 20 de novembro de 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue>DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
```

```

    "glue:UpdateSchema",
    "glue>DeleteSchema",
    "glue:GetSchema",
    "glue:ListSchemas",
    "glue:RegisterSchemaVersion",
    "glue>DeleteSchemaVersions",
    "glue:GetSchemaByDefinition",
    "glue:GetSchemaVersion",
    "glue:GetSchemaVersionsDiff",
    "glue:ListSchemaVersions",
    "glue:CheckSchemaVersionValidity",
    "glue:PutSchemaVersionMetadata",
    "glue:RemoveSchemaVersionMetadata",
    "glue:QuerySchemaVersionMetadata"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetTags",
    "glue:TagResource",
    "glue:UntagResource"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:schema/*",
    "arn:aws:glue:*:*:registry/*"
  ]
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSGlueSchemaRegistryReadOnlyAccess

AWSGlueSchemaRegistryReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao AWS Glue Schema Registry Service

## A utilização desta política

Você pode vincular a AWSGlueSchemaRegistryReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de novembro de 2020, 00:20 UTC
- Horário editado: 20 de novembro de 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
```

```
    "glue:GetSchemaByDefinition",
    "glue:GetSchemaVersion",
    "glue:ListSchemaVersions",
    "glue:GetSchemaVersionsDiff",
    "glue:CheckSchemaVersionValidity",
    "glue:QuerySchemaVersionMetadata",
    "glue:GetTags"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlueServiceNotebookRole

AWSGlueServiceNotebookRole é uma [política AWS gerenciada](#) que: função de serviço Policy for AWS Glue, que permite ao cliente gerenciar o servidor do notebook

### A utilização desta política

Você pode vincular a AWSGlueServiceNotebookRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de agosto de 2017, 13:37 UTC
- Horário editado: 09 de outubro de 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue>DeleteDatabase",
        "glue>DeletePartition",
        "glue>DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue>DeleteConnection",
        "glue>DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",

```

```
    "glue:BatchDeleteConnection",
    "glue:UpdateConnection",
    "glue:GetUserDefinedFunction",
    "glue:UpdateUserDefinedFunction",
    "glue:GetUserDefinedFunctions",
    "glue>DeleteUserDefinedFunction",
    "glue:CreateUserDefinedFunction",
    "glue:BatchGetPartition",
    "glue:BatchDeletePartition",
    "glue:BatchCreatePartition",
    "glue:BatchDeleteTable",
    "glue:UpdateDevEndpoint",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "codewhisperer:GenerateRecommendations"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::crawler-public*",
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue*"
  ]
},
{
  "Effect" : "Allow",
```

```
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "aws-glue-service-resource"
        ]
      }
    },
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGlueServiceRole

AWSGlueServiceRole é uma [política AWS gerenciada](#) que: função de serviço Policy for AWS Glue que permite acesso a serviços relacionados, incluindo EC2, S3 e Cloudwatch Logs

## A utilização desta política

Você pode vincular a `AWSGlueServiceRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço



- Horário de criação: 14 de agosto de 2017, 13:37 UTC
- Horário editado: 11 de setembro de 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*/**",
      "arn:aws:s3:::*/*aws-glue-*/**"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::crawler-public*",
      "arn:aws:s3:::aws-glue-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:*:/aws-glue/*"
    ]
  },
  {
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
},
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*",
  "arn:aws:ec2:*:*:security-group/*",
  "arn:aws:ec2:*:*:instance/*"
]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy é uma [política gerenciada pela AWS](#) que: fornece permissões que permitem que os usuários criem e usem somente as sessões de caderno associadas ao usuário. Essa política também inclui permissões para permitir explicitamente que os usuários passem uma função de sessão restrita do Glue.

## Utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedNotebookPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 18 de abril de 2022, 15:24 UTC
- Horário editado: 22 de novembro de 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
        "owner"
      ]
    }
  },
  {
    "Sid" : "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"
            ]
        }
    }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AwsGlueSessionUserRestrictedNotebookServiceRole

`AwsGlueSessionUserRestrictedNotebookServiceRole` é uma [política AWS gerenciada](#) que: fornece acesso total a todos os recursos do AWS Glue, exceto para sessões. Permite que os usuários criem e usem somente as sessões de caderno que estejam associadas ao usuário. Essa política também inclui outras permissões necessárias para que AWS Glue gerencie os atributos do Glue em outros serviços da AWS.

### A utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedNotebookServiceRole` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 18 de abril de 2022, 15:27 UTC
- Horário editado: 18 de abril de 2022, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```



```
        "owner"
      ]
    }
  },
  {
    "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/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AwsGlueSessionUserRestrictedPolicy

AwsGlueSessionUserRestrictedPolicy é uma [política AWS gerenciada](#) que: fornece permissões que permitem que os usuários criem e usem somente as sessões interativas associadas

ao usuário. Essa política também inclui permissões para permitir explicitamente que os usuários passem uma função de sessão restrita do Glue.

## A utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de abril de 2022, 21:31 UTC
- Horário editado: 14 de abril de 2022, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        }
      },
    }
  ]
}
```

```
    "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:userid}"
      }
    }
  },
  {
    "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" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AwsGlueSessionUserRestrictedServiceRole

`AwsGlueSessionUserRestrictedServiceRole` é uma [política AWS gerenciada](#) que: fornece acesso total a todos os recursos do AWS Glue, exceto para sessões. Permite que os usuários criem e usem somente as sessões interativas associadas ao usuário. Esta política também inclui outras permissões necessárias pelo AWS Glue para gerenciar atributos do Glue em outros serviços da AWS.

## A utilização desta política

Você pode vincular a `AwsGlueSessionUserRestrictedServiceRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de abril de 2022, 21:30 UTC
- Horário editado: 14 de abril de 2022, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*",
    "arn:aws:glue:*:*:tableVersion/*",
    "arn:aws:glue:*:*:connection/*",
    "arn:aws:glue:*:*:userDefinedFunction/*",
    "arn:aws:glue:*:*:devEndpoint/*",
    "arn:aws:glue:*:*:job/*",
    "arn:aws:glue:*:*:trigger/*",
    "arn:aws:glue:*:*:crawler/*",
    "arn:aws:glue:*:*:workflow/*",
    "arn:aws:glue:*:*:mlTransform/*",
    "arn:aws:glue:*:*:registry/*",
    "arn:aws:glue:*:*:schema/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/owner" : "${aws:user}"
    },
    "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:userid}"
      }
    }
  },
  {
    "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/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGrafanaAccountAdministrator

AWSGrafanaAccountAdministrator é uma [política AWS gerenciada](#) que: Fornece acesso ao Amazon Grafana para criar e gerenciar espaços de trabalho para toda a organização.

### A utilização desta política

Você pode vincular a AWSGrafanaAccountAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de fevereiro de 2021, 00:20 UTC
- Horário editado: 15 de fevereiro de 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}
  }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGrafanaConsoleReadOnlyAccess

AWSGrafanaConsoleReadOnlyAccess é uma [política AWS gerenciada](#) que: Acesso a operações somente de leitura no Amazon Grafana.

### A utilização desta política

Você pode vincular a AWSGrafanaConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de fevereiro de 2021, 00:10 UTC
- Horário editado: 15 de fevereiro de 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGrafanaWorkspacePermissionManagement

AWSGrafanaWorkspacePermissionManagement é uma [política AWS gerenciada](#) que: Fornece apenas a capacidade de atualizar as permissões de usuários e grupos para os espaços de trabalho da AWS Grafana.

### A utilização desta política

Você pode vincular a AWSGrafanaWorkspacePermissionManagement aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 23 de fevereiro de 2021, 00:15 UTC
- Horário editado: 15 de março de 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",

```

```
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGrafanaWorkspacePermissionManagementV2

AWSGrafanaWorkspacePermissionManagementV2 é uma [política AWS gerenciada](#) que: Fornece a capacidade de atualizar as permissões de usuários e grupos do IAM Identity Center (iDC) para espaços de trabalho Amazon Managed Grafana.

### Utilização desta política

Você pode vincular a AWSGrafanaWorkspacePermissionManagementV2 aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 05 de janeiro de 2024, 18:39 UTC
- Horário editado: 05 de janeiro de 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

}

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGreengrassFullAccess

AWSGreengrassFullAccess é uma [política AWS gerenciada](#) que: Esta política dá acesso total às ações de configuração, gerenciamento e implantação do AWS Greengrass

### A utilização desta política

Você pode vincular a AWSGreengrassFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de maio de 2017, 00:47 UTC
- Horário editado: 03 de maio de 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGreengrassReadOnlyAccess

AWSGreengrassReadOnlyAccess é uma [política AWS gerenciada](#) que: Esta política fornece acesso somente de leitura às ações de configuração, gerenciamento e implantação do AWS Greengrass

### A utilização desta política

Você pode vincular a AWSGreengrassReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de outubro de 2018, 16:01 UTC

- Horário editado: 30 de outubro de 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSGreengrassResourceAccessRolePolicy

AWSGreengrassResourceAccessRolePolicy é uma [política AWS gerenciada que: Política](#) para a função de serviço do AWS Greengrass, que permite acesso a serviços relacionados, incluindo AWS Lambda e AWS IoT Thing Shadows.

## A utilização desta política

Você pode vincular a AWSGreengrassResourceAccessRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de fevereiro de 2017, 21:17 UTC
- Horário editado: 14 de novembro de 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ]
    }
  ],
}
```

```
"Effect" : "Allow",
"Resource" : [
  "arn:aws:iot:*:*:thing/GG_*",
  "arn:aws:iot:*:*:thing/*-gcm",
  "arn:aws:iot:*:*:thing/*-gda",
  "arn:aws:iot:*:*:thing/*-gci"
]
},
{
  "Sid" : "AllowGreengrassToDescribeThings",
  "Action" : [
    "iot:DescribeThing"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iot:*:*:thing/*"
},
{
  "Sid" : "AllowGreengrassToDescribeCertificates",
  "Action" : [
    "iot:DescribeCertificate"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:iot:*:*:cert/*"
},
{
  "Sid" : "AllowGreengrassToCallGreengrassServices",
  "Action" : [
    "greengrass:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "AllowGreengrassToGetLambdaFunctions",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "AllowGreengrassToGetGreengrassSecrets",
  "Action" : [
```

```
    "secretsmanager:GetSecretValue"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
},
{
  "Sid" : "AllowGreengrassAccessToS3Objects",
  "Action" : [
    "s3:GetObject"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:s3::*Greengrass*",
    "arn:aws:s3::*GreenGrass*",
    "arn:aws:s3::*greengrass*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*sagemaker*"
  ]
},
{
  "Sid" : "AllowGreengrassAccessToS3BucketLocation",
  "Action" : [
    "s3:GetBucketLocation"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
  "Action" : [
    "sagemaker:DescribeTrainingJob"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy é uma [política AWS gerenciada](#) que: Fornece à instância do Dataflow Endpoint permissões para usar o Ground Station Agent AWS

### A utilização desta política

Você pode vincular a AWSGroundStationAgentInstancePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de março de 2023, 15:23 UTC
- Horário editado: 29 de março de 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSHealth\_EventProcessorServiceRolePolicy

AWSHealth\_EventProcessorServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Health habilite o recurso de processador de eventos Health.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de janeiro de 2023, 19:24 UTC
- Horário editado: 13 de janeiro de 2023, 19:24 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSHealthFullAccess

AWSHealthFullAccess é uma [política AWS gerenciada](#) que: Permite acesso total às Apis e Notificações de AWS Saúde e ao Personal Health Dashboard

### A utilização desta política

Você pode vincular a AWSHealthFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de dezembro de 2016, 12:30 UTC
- Horário editado: 16 de novembro de 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Action" : [
  "organizations:EnableAWSServiceAccess",
  "organizations:DisableAWSServiceAccess"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : "health.amazonaws.com"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "health:*",
    "organizations:ListAccounts",
    "organizations:ListParents",
    "organizations:DescribeAccount",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "health.amazonaws.com"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSHealthImagingFullAccess

AWSHealthImagingFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço AWS Health Imaging.

## A utilização desta política

Você pode vincular a AWSHealthImagingFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de julho de 2023, 23:39 UTC
- Horário editado: 25 de julho de 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "medical-imaging.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao serviço AWS Health Imaging.

### A utilização desta política

Você pode vincular a AWSHealthImagingReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de julho de 2023, 23:40 UTC
- Horário editado: 01 de agosto de 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSIAMIdentityCenterAllowListForIdentityContext

AWSIAMIdentityCenterAllowListForIdentityContext é uma [política gerenciada pela AWS](#) que: fornece a lista de ações permitidas para funções assumidas com o contexto de identidade do IAM Identity Center. AWS O Security Token Service (AWSSTS) anexa automaticamente essa política às funções assumidas. O contexto de identidade é passado como ProvidedContext.

## Utilização desta política

Você pode vincular a AWSIAMIdentityCenterAllowListForIdentityContext aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 08 de novembro de 2023, 15:21 UTC
- Horário editado: 25 de novembro de 2023, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total ao serviço Identity Sync

### A utilização desta política

Você pode vincular a AWSIdentitySyncFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de março de 2022, 23:29 UTC
- Horário editado: 23 de março de 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync>DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
```

```
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
    ],
    "Resource" : "arn::*:identity-sync:*:*/*/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIdentitySyncReadOnlyAccess

AWSIdentitySyncReadOnlyAccess é uma [política AWS gerenciada](#) que: Acesso somente de leitura ao serviço Identity Sync

### A utilização desta política

Você pode vincular a AWSIdentitySyncReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de março de 2022, 23:29 UTC
- Horário editado: 23 de março de 2022, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn::*:identity-sync::*:*/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSImageBuilderFullAccess

AWSImageBuilderFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as ações do AWS Image Builder e acesso com escopo de recursos aos AWS serviços relacionados.

## A utilização desta política

Você pode vincular a AWSImageBuilderFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 20 de dezembro de 2019, 18:25 UTC
- Horário editado: 13 de abril de 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*:imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSImageBuilderReadOnlyAccess

AWSImageBuilderReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todas as ações do AWS Image Builder.

### A utilização desta política

Você pode vincular a AWSImageBuilderReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de dezembro de 2019, 22:29 UTC
- Horário editado: 19 de dezembro de 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "imagebuilder:Get*",
      "imagebuilder:List*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/AWSServiceRoleForImageBuilder"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSImportExportFullAccess

`AWSImportExportFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso de leitura e gravação aos trabalhos criados sob Conta da AWS o.

## A utilização desta política

Você pode vincular a `AWSImportExportFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSImportExportReadOnlyAccess

`AWSImportExportReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos trabalhos criados sob Conta da AWS o.

## A utilização desta política

Você pode vincular a `AWSImportExportReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIncidentManagerIncidentAccessServiceRolePolicy

AWSIncidentManagerIncidentAccessServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede permissões ao Incident Manager para chamar outros AWS serviços como parte do gerenciamento de um incidente.

### Utilização desta política

Você pode vincular a AWSIncidentManagerIncidentAccessServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 13 de novembro de 2023, 00:01 UTC
- Horário editado: 20 de fevereiro de 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSIncidentManagerResolverAccess

AWSIncidentManagerResolverAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões para iniciar, visualizar e atualizar incidentes com acesso total a eventos personalizados do cronograma e itens relacionados. Atribua essa política aos usuários que criarão e resolverão incidentes.

### A utilização desta política

Você pode vincular a AWSIncidentManagerResolverAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de maio de 2021, 06:12 UTC
- Horário editado: 10 de maio de 2021, 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "ssm-incidents:ListIncidentRecords",
  "ssm-incidents:GetIncidentRecord",
  "ssm-incidents:UpdateIncidentRecord",
  "ssm-incidents:ListTimelineEvents",
  "ssm-incidents:CreateTimelineEvent",
  "ssm-incidents:GetTimelineEvent",
  "ssm-incidents:UpdateTimelineEvent",
  "ssm-incidents>DeleteTimelineEvent",
  "ssm-incidents:ListRelatedItems",
  "ssm-incidents:UpdateRelatedItems"
],
"Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIncidentManagerServiceRolePolicy

AWSIncidentManagerServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa política concede permissão ao Incident Manager para gerenciar registros de incidentes e recursos relacionados em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço



- Horário de criação: 10 de maio de 2021, 03:34 UTC
- Horário editado: 05 de dezembro de 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IncidentManager"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS IoT 1-Click.

### A utilização desta política

Você pode vincular a AWSIoT1ClickFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2018, 22:10 UTC
- Horário editado: 11 de maio de 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao AWS IoT 1-Click.

## A utilização desta política

Você pode vincular a AWSIoT1ClickReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de maio de 2018, 21:49 UTC
- Horário editado: 11 de maio de 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTAnalyticsFullAccess

AWSIoTAnalyticsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao IoT Analytics.

### A utilização desta política

Você pode vincular a AWSIoTAnalyticsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de junho de 2018, 23:02 UTC
- Horário editado: 18 de junho de 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTAnalyticsReadOnlyAccess

AWSIoTAnalyticsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao IoT Analytics.

### A utilização desta política

Você pode vincular a AWSIoTAnalyticsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 18 de junho de 2018, 21:37 UTC
- Horário editado: 18 de junho de 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTConfigAccess

AWSIoTConfigAccess é uma [política AWS gerenciada](#) que: Essa política dá acesso total às ações de configuração de AWS IoT

### A utilização desta política

Você pode vincular a AWSIoTConfigAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de outubro de 2015, 21:52 UTC

- Horário editado: 27 de setembro de 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

## Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
```



```
"iot:DeleteAuthorizer",
"iot:DeleteCACertificate",
"iot:DeleteCertificate",
"iot:DeleteJob",
"iot:DeleteJobExecution",
"iot:DeleteOTAUpdate",
"iot:DeletePolicy",
"iot:DeletePolicyVersion",
"iot:DeleteRegistrationCode",
"iot:DeleteRoleAlias",
"iot:DeleteStream",
"iot:DeleteThing",
"iot:DeleteThingGroup",
"iot:DeleteThingType",
"iot:DeleteTopicRule",
"iot:DeleteV2LoggingLevel",
"iot:DeprecateThingType",
"iot:DescribeAuthorizer",
"iot:DescribeCACertificate",
"iot:DescribeCertificate",
"iot:DescribeDefaultAuthorizer",
"iot:DescribeEndpoint",
"iot:DescribeEventConfigurations",
"iot:DescribeIndex",
"iot:DescribeJob",
"iot:DescribeJobExecution",
"iot:DescribeRoleAlias",
"iot:DescribeStream",
"iot:DescribeThing",
"iot:DescribeThingGroup",
"iot:DescribeThingRegistrationTask",
"iot:DescribeThingType",
"iot:DetachPolicy",
"iot:DetachPrincipalPolicy",
"iot:DetachThingPrincipal",
"iot:DisableTopicRule",
"iot:EnableTopicRule",
"iot:GetEffectivePolicies",
"iot:GetIndexingConfiguration",
"iot:GetJobDocument",
"iot:GetLoggingOptions",
"iot:GetOTAUpdate",
"iot:GetPolicy",
"iot:GetPolicyVersion",
```

```
"iot:GetRegistrationCode",
"iot:GetTopicRule",
"iot:GetV2LoggingOptions",
"iot:ListAttachedPolicies",
"iot:ListAuthorizers",
"iot:ListCACertificates",
"iot:ListCertificates",
"iot:ListCertificatesByCA",
"iot:ListIndices",
"iot:ListJobExecutionsForJob",
"iot:ListJobExecutionsForThing",
"iot:ListJobs",
"iot:ListOTAUpdates",
"iot:ListOutgoingCertificates",
"iot:ListPolicies",
"iot:ListPolicyPrincipals",
"iot:ListPolicyVersions",
"iot:ListPrincipalPolicies",
"iot:ListPrincipalThings",
"iot:ListRoleAliases",
"iot:ListStreams",
"iot:ListTargetsForPolicy",
"iot:ListThingGroups",
"iot:ListThingGroupsForThing",
"iot:ListThingPrincipals",
"iot:ListThingRegistrationTaskReports",
"iot:ListThingRegistrationTasks",
"iot:ListThings",
"iot:ListThingsInThingGroup",
"iot:ListThingTypes",
"iot:ListTopicRules",
"iot:ListV2LoggingLevels",
"iot:RegisterCACertificate",
"iot:RegisterCertificate",
"iot:RegisterThing",
"iot:RejectCertificateTransfer",
"iot:RemoveThingFromThingGroup",
"iot:ReplaceTopicRule",
"iot:SearchIndex",
"iot:SetDefaultAuthorizer",
"iot:SetDefaultPolicyVersion",
"iot:SetLoggingOptions",
"iot:SetV2LoggingLevel",
"iot:SetV2LoggingOptions",
```

```
    "iot:StartThingRegistrationTask",
    "iot:StopThingRegistrationTask",
    "iot:TestAuthorization",
    "iot:TestInvokeAuthorizer",
    "iot:TransferCertificate",
    "iot:UpdateAuthorizer",
    "iot:UpdateCACertificate",
    "iot:UpdateCertificate",
    "iot:UpdateEventConfigurations",
    "iot:UpdateIndexingConfiguration",
    "iot:UpdateRoleAlias",
    "iot:UpdateStream",
    "iot:UpdateThing",
    "iot:UpdateThingGroup",
    "iot:UpdateThingGroupsForThing",
    "iot:UpdateAccountAuditConfiguration",
    "iot:DescribeAccountAuditConfiguration",
    "iot>DeleteAccountAuditConfiguration",
    "iot:StartOnDemandAuditTask",
    "iot:CancelAuditTask",
    "iot:DescribeAuditTask",
    "iot>ListAuditTasks",
    "iot>CreateScheduledAudit",
    "iot:UpdateScheduledAudit",
    "iot>DeleteScheduledAudit",
    "iot:DescribeScheduledAudit",
    "iot>ListScheduledAudits",
    "iot>ListAuditFindings",
    "iot>CreateSecurityProfile",
    "iot:DescribeSecurityProfile",
    "iot:UpdateSecurityProfile",
    "iot>DeleteSecurityProfile",
    "iot:AttachSecurityProfile",
    "iot:DetachSecurityProfile",
    "iot>ListSecurityProfiles",
    "iot>ListSecurityProfilesForTarget",
    "iot>ListTargetsForSecurityProfile",
    "iot>ListActiveViolations",
    "iot>ListViolationEvents",
    "iot:ValidateSecurityProfileBehaviors"
  ],
  "Resource" : "*"
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTConfigReadOnlyAccess

AWSIoTConfigReadOnlyAccess é uma [política AWS gerenciada](#) que: Essa política fornece acesso somente de leitura às ações de configuração de AWS IoT

### A utilização desta política

Você pode vincular a AWSIoTConfigReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de outubro de 2015, 21:52 UTC
- Horário editado: 27 de setembro de 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeAuthorizer",
      "iot:DescribeCACertificate",
      "iot:DescribeCertificate",
      "iot:DescribeDefaultAuthorizer",
      "iot:DescribeEndpoint",
      "iot:DescribeEventConfigurations",
      "iot:DescribeIndex",
      "iot:DescribeJob",
      "iot:DescribeJobExecution",
      "iot:DescribeRoleAlias",
      "iot:DescribeStream",
      "iot:DescribeThing",
      "iot:DescribeThingGroup",
      "iot:DescribeThingRegistrationTask",
      "iot:DescribeThingType",
      "iot:GetEffectivePolicies",
      "iot:GetIndexingConfiguration",
      "iot:GetJobDocument",
      "iot:GetLoggingOptions",
      "iot:GetOTAUpdate",
      "iot:GetPolicy",
      "iot:GetPolicyVersion",
      "iot:GetRegistrationCode",
      "iot:GetTopicRule",
      "iot:GetV2LoggingOptions",
      "iot:ListAttachedPolicies",
      "iot:ListAuthorizers",
      "iot:ListCACertificates",
      "iot:ListCertificates",
      "iot:ListCertificatesByCA",
      "iot:ListIndices",
      "iot:ListJobExecutionsForJob",
      "iot:ListJobExecutionsForThing",
      "iot:ListJobs",
      "iot:ListOTAUpdates",
      "iot:ListOutgoingCertificates",
      "iot:ListPolicies",
      "iot:ListPolicyPrincipals",
      "iot:ListPolicyVersions",
```

```
    "iot:ListPrincipalPolicies",
    "iot:ListPrincipalThings",
    "iot:ListRoleAliases",
    "iot:ListStreams",
    "iot:ListTargetsForPolicy",
    "iot:ListThingGroups",
    "iot:ListThingGroupsForThing",
    "iot:ListThingPrincipals",
    "iot:ListThingRegistrationTaskReports",
    "iot:ListThingRegistrationTasks",
    "iot:ListThings",
    "iot:ListThingsInThingGroup",
    "iot:ListThingTypes",
    "iot:ListTopicRules",
    "iot:ListV2LoggingLevels",
    "iot:SearchIndex",
    "iot:TestAuthorization",
    "iot:TestInvokeAuthorizer",
    "iot:DescribeAccountAuditConfiguration",
    "iot:DescribeAuditTask",
    "iot:ListAuditTasks",
    "iot:DescribeScheduledAudit",
    "iot:ListScheduledAudits",
    "iot:ListAuditFindings",
    "iot:DescribeSecurityProfile",
    "iot:ListSecurityProfiles",
    "iot:ListSecurityProfilesForTarget",
    "iot:ListTargetsForSecurityProfile",
    "iot:ListActiveViolations",
    "iot:ListViolationEvents",
    "iot:ValidateSecurityProfileBehaviors"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDataAccess

AWSIoTDataAccess é uma [política AWS gerenciada](#) que: Essa política dá acesso total às ações de mensagens de AWS IoT

### A utilização desta política

Você pode vincular a AWSIoTDataAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de outubro de 2015, 21:51 UTC
- Horário editado: 23 de junho de 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
```

```
    "iot:Receive",
    "iot:GetThingShadow",
    "iot:UpdateThingShadow",
    "iot:DeleteThingShadow",
    "iot:ListNamedShadowsForThing"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` é uma [política AWS gerenciada](#) que: fornece acesso de gravação a grupos de coisas de IoT e acesso de leitura a certificados de IoT para execução da ação de mitigação `ADD_THINGS_TO_THING_GROUP`

### A utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de agosto de 2019, 17:55 UTC
- Horário editado: 07 de agosto de 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderAudit

AWSIoTDeviceDefenderAudit é uma [política AWS gerenciada](#) que: Fornece acesso de leitura para IoT e recursos relacionados

## A utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderAudit` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 18 de julho de 2018, 21:17 UTC
- Horário editado: 25 de novembro de 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",

```

```
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies",
    "iam:GetRole",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRolePolicy",
    "iam:GenerateServiceLastAccessedDetails",
    "iam:GetServiceLastAccessedDetails"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction é uma [política AWS gerenciada](#) que: Fornece acesso para habilitar o registro de IoT para execução da ação de mitigação ENABLE\_IOT\_LOGGING

### A utilização desta política

Você pode vincular a AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço

- Horário de criação: 07 de agosto de 2019, 17:04 UTC
- Horário editado: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction é uma [política AWS gerenciada](#) que: Fornece acesso de publicação de mensagens ao tópico SNS para execução da ação de mitigação PUBLISH\_FINDING\_TO\_SNS

### A utilização desta política

Você pode vincular a AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de agosto de 2019, 17:04 UTC
- Horário editado: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` é uma [política AWS gerenciada](#) que: Fornece acesso de gravação às políticas de IoT para execução da ação de mitigação `REPLACE_DEFAULT_POLICY_VERSION`

## A utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de agosto de 2019, 17:04 UTC
- Horário editado: 07 de agosto de 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction é uma [política AWS gerenciada](#) que: Fornece acesso de gravação aos certificados de CA de IoT para execução da ação de mitigação UPDATE\_CA\_CERTIFICATE

### A utilização desta política

Você pode vincular a AWSIoTDeviceDefenderUpdateCACertMitigationAction aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de agosto de 2019, 17:05 UTC
- Horário editado: 07 de agosto de 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Effect" : "Allow",
    "Action" : [
      "iot:UpdateCACertificate"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` é uma [política AWS gerenciada](#) que: Fornece acesso de gravação aos certificados de IoT para execução da ação de mitigação `UPDATE_DEVICE_CERTIFICATE`

### A utilização desta política

Você pode vincular a `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de agosto de 2019, 17:06 UTC
- Horário editado: 07 de agosto de 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceTesterForFreeRTOSFullAccess

AWSIoTDeviceTesterForFreeRTOSFullAccess é uma [política AWS gerenciada](#) que: Permite que o AWS IoT Device Tester execute o pacote de qualificação do FreeRTOS, permitindo acesso a serviços, incluindo IoT, S3 e IAM

## A utilização desta política

Você pode vincular a `AWSIoTDeviceTesterForFreeRTOSFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de fevereiro de 2020, 20:33 UTC
- Horário editado: 10 de agosto de 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
```

```

    "iot:DeleteThing",
    "iot:AttachThingPrincipal",
    "iot:DeleteCertificate",
    "iot:GetRegistrationCode",
    "iot:CreatePolicy",
    "iot:UpdateCACertificate",
    "s3:ListBucket",
    "iot:DescribeEndpoint",
    "iot:CreateOTAUpdate",
    "iot:CreateStream",
    "signer:ListSigningJobs",
    "acm:ListCertificates",
    "iot:CreateKeysAndCertificate",
    "iot:UpdateCertificate",
    "iot:CreateCertificateFromCsr",
    "iot:DetachThingPrincipal",
    "iot:RegisterCACertificate",
    "iot:CreateThing",
    "iam:ListRoles",
    "iot:RegisterCertificate",
    "iot:DeleteCACertificate",
    "signer:PutSigningProfile",
    "s3:ListAllMyBuckets",
    "signer:ListSigningPlatforms",
    "iot-device-tester:SendMetrics",
    "iot-device-tester:SupportedVersion",
    "iot-device-tester:LatestIdt",
    "iot-device-tester:CheckVersion",
    "iot-device-tester:DownloadTestSuite"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor2",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "signer:StartSigningJob",
    "acm:GetCertificate",
    "signer:DescribeSigningJob",
    "s3:CreateBucket",
    "execute-api:Invoke",
    "s3>DeleteBucket",
    "s3:PutBucketVersioning",

```

```
    "signer:CancelSigningProfile"
  ],
  "Resource" : [
    "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
    "arn:aws:signer:*:*:/signing-profiles/*",
    "arn:aws:signer:*:*:/signing-jobs/*",
    "arn:aws:iam:*:*:role/idt-*",
    "arn:aws:acm:*:*:certificate/*",
    "arn:aws:s3:::idt-*",
    "arn:aws:s3:::afr-ota*"
  ]
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",
  "Action" : [
    "iot:DeleteStream",
    "iot:DeleteCertificate",
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "iot:DeletePolicy",
    "s3:ListBucketVersions",
    "iot:UpdateCertificate",
    "iot:GetOTAUpdate",
    "iot:DeleteOTAUpdate",
    "iot:DescribeJobExecution"
  ],
  "Resource" : [
    "arn:aws:s3:::afr-ota*",
    "arn:aws:iot:*:*:thinggroup/idt*",
    "arn:aws:iam:*:*:role/idt-*"
  ]
},
{
  "Sid" : "VisualEditor4",
  "Effect" : "Allow",
  "Action" : [
    "iot:DeleteCertificate",
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "s3:DeleteObjectVersion",
    "iot:DeleteOTAUpdate",
    "s3:PutObject",
    "s3:GetObject",
```

```

    "iot:DeleteStream",
    "iot:DeletePolicy",
    "s3:DeleteObject",
    "iot:UpdateCertificate",
    "iot:GetOTAUpdate",
    "s3:GetObjectVersion",
    "iot:DescribeJobExecution"
  ],
  "Resource" : [
    "arn:aws:s3:::afr-ota*/**",
    "arn:aws:s3:::idt-*/**",
    "arn:aws:iot:*:*:policy/idt*",
    "arn:aws:iam:*:*:role/idt-*",
    "arn:aws:iot:*:*:otaupdate/idt*",
    "arn:aws:iot:*:*:thing/idt*",
    "arn:aws:iot:*:*:cert/**",
    "arn:aws:iot:*:*:job/**",
    "arn:aws:iot:*:*:stream/**"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::afr-ota*/**",
    "arn:aws:s3:::idt-*/**"
  ]
},
{
  "Sid" : "VisualEditor6",
  "Effect" : "Allow",
  "Action" : [
    "iot:CancelJobExecution"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/**",
    "arn:aws:iot:*:*:thing/idt*"
  ]
},
{

```

```
"Sid" : "VisualEditor7",
"Effect" : "Allow",
"Action" : [
  "ec2:TerminateInstances"
],
"Resource" : [
  "arn:aws:ec2:*:*:instance/*"
],
"Condition" : {
  "StringEquals" : {
    "ec2:ResourceTag/Owner" : "IoTDeviceTester"
  }
}
},
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor9",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
}
```

```
},
{
  "Sid" : "VisualEditor10",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "VisualEditor11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Owner" : "IoTDeviceTester"
    }
  }
},
{
  "Sid" : "VisualEditor12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ssm:DescribeParameters",
    "ssm:GetParameters"
  ],
  "Resource" : "*"
},
```



```
{
  "Sid" : "VisualEditor13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "Owner"
      ]
    },
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateSecurityGroup"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTDeviceTesterForGreengrassFullAccess

AWSIoTDeviceTesterForGreengrassFullAccess é uma [política AWS gerenciada](#) que: Permite que o AWS IoT Device Tester execute o pacote de qualificação AWS Greengrass, permitindo acesso a serviços relacionados, incluindo Lambda, IoT, API Gateway, IAM

## A utilização desta política

Você pode vincular a `AWSIoTDeviceTesterForGreengrassFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de fevereiro de 2020, 21:21 UTC
- Horário editado: 25 de junho de 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
    }
  ],
},
```

```
{
  "Sid" : "VisualEditor2",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "iot>DeleteCertificate",
    "lambda>DeleteFunction",
    "execute-api:Invoke",
    "iot:UpdateCertificate"
  ],
  "Resource" : [
    "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
    "arn:aws:lambda:*:*:function:idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor3",
  "Effect" : "Allow",
  "Action" : [
    "iot>CreateThing",
    "iot>DeleteThing"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor4",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachPolicy",
    "iot:DetachPolicy",
    "iot>DeletePolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/idt-*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "VisualEditor5",
  "Effect" : "Allow",
```

```

    "Action" : [
      "iot:CreateJob",
      "iot:DescribeJob",
      "iot:DescribeJobExecution",
      "iot>DeleteJob"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:thing/idt-*",
      "arn:aws:iot:*:*:job/*"
    ]
  },
  {
    "Sid" : "VisualEditor6",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeEndpoint",
      "greengrass:*",
      "iam:ListAttachedRolePolicies",
      "iot:CreatePolicy",
      "iot:GetThingShadow",
      "iot:CreateKeysAndCertificate",
      "iot:ListThings",
      "iot:UpdateThingShadow",
      "iot:CreateCertificateFromCsr",
      "iot-device-tester:SendMetrics",
      "iot-device-tester:SupportedVersion",
      "iot-device-tester:LatestIdt",
      "iot-device-tester:CheckVersion",
      "iot-device-tester:DownloadTestSuite"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VisualEditor7",
    "Effect" : "Allow",
    "Action" : [
      "iot:DetachThingPrincipal",
      "iot:AttachThingPrincipal"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:thing/idt-*",
      "arn:aws:iot:*:*:cert/*"
    ]
  },

```

```
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject",
    "s3:DeleteObjectVersion",
    "s3:ListBucketVersions",
    "s3:CreateBucket",
    "s3:DeleteObject",
    "s3:DeleteBucket"
  ],
  "Resource" : "arn:aws:s3:::idt*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTEventsFullAccess

AWSIoTEventsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos eventos de IoT.

### A utilização desta política

Você pode vincular a AWSIoTEventsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de janeiro de 2019, 22:51 UTC
- Horário editado: 10 de janeiro de 2019, 22:51 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTEventsReadOnlyAccess

`AWSIoTEventsReadOnlyAccess` é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao IoT Events.

## A utilização desta política

Você pode vincular a `AWSIoTEventsReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 10 de janeiro de 2019, 22:50 UTC
- Horário editado: 23 de setembro de 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoT FleetHubFederationAccess

AWSIoT FleetHubFederationAccess é uma [política AWS gerenciada](#) que: Acesso à federação para aplicativos IoT Fleet Hub

### A utilização desta política

Você pode vincular a AWSIoT FleetHubFederationAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 15 de dezembro de 2020, 08:08 UTC
- Horário editado: 04 de abril de 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "iot:GetBucketsAggregation",
    "iot:GetCardinality",
    "iot:GetIndexingConfiguration",
    "iot:GetPercentiles",
    "iot:GetStatistics",
    "iot:SearchIndex",
    "iot:CreateFleetMetric",
    "iot:ListFleetMetrics",
    "iot>DeleteFleetMetric",
    "iot:DescribeFleetMetric",
    "iot:UpdateFleetMetric",
    "iot:DescribeCustomMetric",
    "iot:ListCustomMetrics",
    "iot:ListDimensions",
    "iot:ListMetricValues",
    "iot:ListThingGroups",
    "iot:ListThingsInThingGroup",
    "iot:ListJobTemplates",
    "iot:DescribeJobTemplate",
    "iot:ListJobs",
    "iot:CreateJob",
    "iot:CancelJob",
    "iot:DescribeJob",
    "iot:ListJobExecutionsForJob",
    "iot:ListJobExecutionsForThing",
    "iot:DescribeJobExecution",
    "iot:ListSecurityProfiles",
    "iot:DescribeSecurityProfile",
    "iot:ListActiveViolations",
    "iot:GetThingShadow",
    "iot:ListNamedShadowsForThing",
    "iot:CancelJobExecution",
    "iot:DescribeEndpoint",
    "iotfleethub:DescribeApplication",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "sns:ListTopics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
```

```
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
    ],
    "Resource" : "arn:aws:sns:*:*:iotfleethub*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoT Fleetwise Service Role Policy

AWSIoT Fleetwise Service Role Policy é uma [política AWS gerenciada](#) que: Concede permissões a AWS recursos e metadados usados ou gerenciados pelo AWSIoT Fleetwise para recursos auxiliares

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de setembro de 2022, 23:27 UTC
- Horário editado: 21 de setembro de 2022, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT FleetwiseServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTFullAccess

`AWSIoTFullAccess` é uma [política AWS gerenciada](#) que: Essa política dá acesso total às ações de configuração e mensagens de AWS IoT

### A utilização desta política

Você pode vincular a `AWSIoTFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de outubro de 2015, 15:19 UTC
- Horário editado: 19 de maio de 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Action" : [
      "iot:*",
      "iotjobsdata:*"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTLogging

AWSIoTLogging é uma [política AWS gerenciada](#) que: Permite a criação de grupos do Amazon CloudWatch Log e streaming de logs para os grupos

### A utilização desta política

Você pode vincular a AWSIoTLogging aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 08 de outubro de 2015, 15:17 UTC
- Horário editado: 08 de outubro de 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTOTAUpdate

AWSIoTOTAUpdate é uma [política AWS gerenciada](#) que: Permite o acesso para criar um AWS IoT Job e descrever o trabalho do assinante de AWS código

## A utilização desta política

Você pode vincular a `AWSIoTOTAUpdate` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de dezembro de 2017, 20:36 UTC
- Horário editado: 20 de dezembro de 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTRoboRunnerFullAccess

`AWSIoTRoboRunnerFullAccess` é uma [política AWS gerenciada](#) que: Essa política concede permissões que permitem acesso total ao AWS IoT RoboRunner.

### A utilização desta política

Você pode vincular a `AWSIoTRoboRunnerFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 03:54 UTC
- Horário editado: 23 de fevereiro de 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/AWSServiceRoleForIoTRoboRunner",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTRoboRunnerReadOnly

`AWSIoTRoboRunnerReadOnly` é uma [política AWS gerenciada](#) que: Esta política concede permissões que oferecem acesso somente leitura ao AWS IoT RoboRunner.

### A utilização desta política

Você pode vincular a `AWSIoTRoboRunnerReadOnly` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 03:43 UTC
- Horário editado: 16 de novembro de 2022, 20:51 UTC

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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSIoTRoboRunnerServiceRolePolicy

`AWSIoTRoboRunnerServiceRolePolicy` é uma [política AWS gerenciada](#) que: Permite que o AWS IoT RoboRunner gerencie os AWS recursos associados em nome do cliente.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de fevereiro de 2023, 16:56 UTC
- Horário editado: 21 de fevereiro de 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
```

```
    "cloudwatch:namespace" : [  
      "AWS/Usage"  
    ]  
  }  
}  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTRuleActions

AWSIoTRuleActions é uma [política AWS gerenciada](#) que: Permite acesso a todos os AWS serviços suportados nas ações de regras de AWS IoT

## A utilização desta política

Você pode vincular a AWSIoTRuleActions aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 08 de outubro de 2015, 15:14 UTC
- Horário editado: 16 de janeiro de 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
  }
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTSiteWiseConsoleFullAccess

`AWSIoTSiteWiseConsoleFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total para gerenciar o AWS IoT SiteWise usando o. AWS Management Console Observe que essa política também concede acesso para criar e listar armazenamentos de dados usados com o AWS IoT SiteWise (AWSpor exemplo, IoT Analytics), acesso para listar e AWS visualizar recursos do IoT Greengrass, listar e AWS modificar segredos do Secrets Manager, recuperar sombras de coisas da

IoT, listar recursos com tags específicas e criar e usar uma função vinculada a serviços para o IoT SiteWise. AWS AWS

## A utilização desta política

Você pode vincular a `AWSIoTSiteWiseConsoleFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 31 de maio de 2019, 21:37 UTC
- Horário editado: 31 de maio de 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
  },
  {
    "Action" : [
      "iot:DescribeEndpoint",
      "iot:GetThingShadow"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "greengrass:GetGroup",
      "greengrass:GetGroupVersion",
      "greengrass:GetCoreDefinitionVersion",
      "greengrass:ListGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "secretsmanager:ListSecrets",
      "secretsmanager:CreateSecret"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "secretsmanager:UpdateSecret"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
  },
  {
    "Action" : [
      "tag:GetResources"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ]
  }
}
```

```
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
      }
    }
  },
  {
    "Action" : [
      "iam:PassRole"
    ],
    "Effect" : "Allow",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "iotsitewise.amazonaws.com"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTSiteWiseFullAccess

AWSIoTSiteWiseFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao IoT SiteWise.



## A utilização desta política

Você pode vincular a `AWSIoTSiteWiseFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de dezembro de 2018, 20:53 UTC
- Horário editado: 04 de dezembro de 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTSiteWiseMonitorPortalAccess

AWSIoTSiteWiseMonitorPortalAccess é uma [política AWS gerenciada](#) que: [Essa política](#) concede permissões para acessar ativos e dados de ativos do AWS IoT SiteWise, criar recursos do IoT SiteWise AWS Monitor e listar usuários de SSO. AWS

### A utilização desta política

Você pode vincular a AWSIoTSiteWiseMonitorPortalAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 19 de maio de 2020, 20:01 UTC
- Horário editado: 19 de maio de 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iotsitewise:CreateProject",
    "iotsitewise:DescribeProject",
    "iotsitewise:UpdateProject",
    "iotsitewise>DeleteProject",
    "iotsitewise:ListProjects",
    "iotsitewise:BatchAssociateProjectAssets",
    "iotsitewise:BatchDisassociateProjectAssets",
    "iotsitewise:ListProjectAssets",
    "iotsitewise:CreateDashboard",
    "iotsitewise:DescribeDashboard",
    "iotsitewise:UpdateDashboard",
    "iotsitewise>DeleteDashboard",
    "iotsitewise:ListDashboards",
    "iotsitewise:CreateAccessPolicy",
    "iotsitewise:DescribeAccessPolicy",
    "iotsitewise:UpdateAccessPolicy",
    "iotsitewise>DeleteAccessPolicy",
    "iotsitewise:ListAccessPolicies",
    "iotsitewise:DescribeAsset",
    "iotsitewise:ListAssets",
    "iotsitewise:ListAssociatedAssets",
    "iotsitewise:DescribeAssetProperty",
    "iotsitewise:GetAssetPropertyValue",
    "iotsitewise:GetAssetPropertyValueHistory",
    "iotsitewise:GetAssetPropertyAggregates",
    "sso-directory:DescribeUsers"
  ],
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSIoTSiteWiseMonitorServiceRolePolicy

AWSIoTSiteWiseMonitorServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa função concede permissões de monitor AWS ao IoT SiteWise para acessar seus ativos e propriedades de ativos do AWS IoT SiteWise e AWS criar projetos, painéis e políticas de acesso do IoT SiteWise por meio dos portais do IoT SiteWise. AWS

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de novembro de 2019, 00:59 UTC
- Horário editado: 13 de dezembro de 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

    "iotsitewise:DescribeProject",
    "iotsitewise:UpdateProject",
    "iotsitewise>DeleteProject",
    "iotsitewise:ListProjects",
    "iotsitewise:BatchAssociateProjectAssets",
    "iotsitewise:BatchDisassociateProjectAssets",
    "iotsitewise:ListProjectAssets",
    "iotsitewise:CreateDashboard",
    "iotsitewise:DescribeDashboard",
    "iotsitewise:UpdateDashboard",
    "iotsitewise>DeleteDashboard",
    "iotsitewise:ListDashboards",
    "iotsitewise:CreateAccessPolicy",
    "iotsitewise:DescribeAccessPolicy",
    "iotsitewise:UpdateAccessPolicy",
    "iotsitewise>DeleteAccessPolicy",
    "iotsitewise:ListAccessPolicies",
    "iotsitewise:DescribeAsset",
    "iotsitewise:ListAssets",
    "iotsitewise:ListAssociatedAssets",
    "iotsitewise:DescribeAssetProperty",
    "iotsitewise:GetAssetPropertyValue",
    "iotsitewise:GetAssetPropertyValueHistory",
    "iotsitewise:GetAssetPropertyAggregates",
    "sso-directory:DescribeUsers"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTSiteWiseReadOnlyAccess

`AWSIoTSiteWiseReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao IoT SiteWise.

## A utilização desta política

Você pode vincular a `AWSIoTSiteWiseReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de dezembro de 2018, 20:55 UTC
- Horário editado: 16 de setembro de 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTThingsRegistration

AWSIoTThingsRegistration é uma [política AWS gerenciada que: Essa política](#) permite que os usuários registrem coisas em massa usando a API AWS IoT StartthingRegistrationTask

### A utilização desta política

Você pode vincular a AWSIoTThingsRegistration aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de dezembro de 2017, 20:21 UTC
- Horário editado: 05 de outubro de 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "iot:AddThingToThingGroup",
    "iot:AttachPolicy",
    "iot:AttachPrincipalPolicy",
    "iot:AttachThingPrincipal",
    "iot:CreateCertificateFromCsr",
    "iot:CreatePolicy",
    "iot:CreateThing",
    "iot:DescribeCertificate",
    "iot:DescribeThing",
    "iot:DescribeThingGroup",
    "iot:DescribeThingType",
    "iot:DetachPolicy",
    "iot:DetachThingPrincipal",
    "iot:GetPolicy",
    "iot:ListAttachedPolicies",
    "iot:ListPolicyPrincipals",
    "iot:ListPrincipalPolicies",
    "iot:ListPrincipalThings",
    "iot:ListTargetsForPolicy",
    "iot:ListThingGroupsForThing",
    "iot:ListThingPrincipals",
    "iot:RegisterCertificate",
    "iot:RegisterThing",
    "iot:RemoveThingFromThingGroup",
    "iot:UpdateCertificate",
    "iot:UpdateThing",
    "iot:UpdateThingGroupsForThing",
    "iot:AddThingToBillingGroup",
    "iot:DescribeBillingGroup",
    "iot:RemoveThingFromBillingGroup"
  ],
  "Resource" : [
    "*"
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTtwinMakerServiceRolePolicy

AWSIoTtwinMakerServiceRolePolicy é uma [política AWS gerenciada](#) que: permite que TwinMaker a AWS IoT chame outros AWS serviços e sincronize seus recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de novembro de 2023, 18:59 UTC
- Hora da edição: 13 de novembro de 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",

```

```
    "iottwinmaker:DeleteEntity",
    "iottwinmaker:ListEntities",
    "iottwinmaker:GetComponentType",
    "iottwinmaker:CreateComponentType",
    "iottwinmaker:UpdateComponentType",
    "iottwinmaker>DeleteComponentType",
    "iottwinmaker:ListComponentTypes"
  ],
  "Resource" : [
    "arn:aws:iottwinmaker:*:*:workspace/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "iottwinmaker:linkedServices" : [
        "IOTSITWISE"
      ]
    }
  }
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTWirelessDataAccess

AWSIoTWirelessDataAccess é uma [política AWS gerenciada](#) que: Permite que os dados de identidade associados acessem dispositivos AWS IoT Wireless.

### A utilização desta política

Você pode vincular a AWSIoTWirelessDataAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 15 de dezembro de 2020, 15:31 UTC
- Horário editado: 15 de dezembro de 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSIoTWirelessFullAccess

AWSIoTWirelessFullAccess é uma [política AWS gerenciada](#) que: Permite que a identidade associada tenha acesso total a todas as operações AWS do IoT Wireless.

## A utilização desta política

Você pode vincular a AWSIoTWirelessFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 15:27 UTC
- Horário editado: 15 de dezembro de 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTWirelessFullPublishAccess

AWSIoTWirelessFullPublishAccess é uma [política AWS gerenciada](#) que: Fornece à IoT Wireless acesso total para publicar no IoT Rules Engine em seu nome.

### A utilização desta política

Você pode vincular a AWSIoTWirelessFullPublishAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 15:29 UTC
- Horário editado: 15 de dezembro de 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTWirelessGatewayCertManager

AWSIoTWirelessGatewayCertManager é uma [política AWS gerenciada](#) que: Permite o acesso à identidade associada para criar, listar e descrever certificados de IoT

### A utilização desta política

Você pode vincular a AWSIoTWirelessGatewayCertManager aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 15:30 UTC
- Horário editado: 15 de dezembro de 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTWirelessLogging

AWSIoTWirelessLogging é uma [política AWS gerenciada](#) que: Permite que a identidade associada crie grupos do Amazon CloudWatch Logs e transmita logs para os grupos.



## A utilização desta política

Você pode vincular a `AWSIoTWirelessLogging` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 15:32 UTC
- Horário editado: 15 de dezembro de 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIoTWirelessReadOnlyAccess

AWSIoTWirelessReadOnlyAccess é uma [política AWS gerenciada](#) que: Permite que a identidade associada tenha acesso somente para leitura à AWS IoT sem fio.

### A utilização desta política

Você pode vincular a AWSIoTWirelessReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de dezembro de 2020, 15:28 UTC
- Horário editado: 15 de dezembro de 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iotwireless:List*",
      "iotwireless:Get*"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIPAMServiceRolePolicy

AWSIPAMServiceRolePolicy é uma [política gerenciada pela AWS](#) que: permite que o VPC IP Address Manager acesse os recursos da VPC e se integre às AWS Organizations em seu nome.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de novembro de 2021, 19:08 UTC
- Hora da edição: 08 de novembro de 2023, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
```

```
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/IPAM"
      }
    }
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy é uma [política AWS gerenciada](#) que: Usada pelo AWS IQ para executar solicitações de pagamento em nome de um cliente

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 22 de agosto de 2019, 19:28 UTC
- Horário editado: 22 de agosto de 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIQFullAccess

AWSIQFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS IQ

## A utilização desta política

Você pode vincular a AWSIQFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de abril de 2019, 23:13 UTC
- Horário editado: 25 de setembro de 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSIQPermissionServiceRolePolicy

AWSIQPermissionServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS IQ gerencie a função assumida pelos especialistas em QIAWS.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 22 de agosto de 2019, 19:36 UTC
- Horário editado: 22 de agosto de 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteRole",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
    "Condition" : {
      "ArnEquals" : {
        "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DetachRolePolicy"
    ],
    "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy é uma [política gerenciada pela AWS](#) que: permite o acesso aos serviços e recursos da AWS necessários para os armazenamentos de chaves personalizadas do AWS KMS

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de novembro de 2018, 20:10 UTC
- Hora da edição: 10 de novembro de 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS KMS sincronize as propriedades compartilhadas das chaves multirregionais.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de junho de 2021, 15:37 UTC
- Horário editado: 16 de junho de 2021, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSKeyManagementServicePowerUser

AWSKeyManagementServicePowerUser é uma [política AWS gerenciada](#) que: Fornece acesso ao AWS Key Management Service (KMS).

## A utilização desta política

Você pode vincular a AWSKeyManagementServicePowerUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 07 de março de 2017, 00:55 UTC

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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms>DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLakeFormationCrossAccountManager

`AWSLakeFormationCrossAccountManager` é uma [política AWS gerenciada](#) que: Fornece acesso entre contas aos recursos do Glue por meio do Lake Formation. Também concede acesso de leitura a outros serviços necessários, como organizações e gerenciador de acesso a recursos

### A utilização desta política

Você pode vincular a `AWSLakeFormationCrossAccountManager` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de agosto de 2020, 20:59 UTC
- Horário editado: 01 de novembro de 2023, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "ram:CreateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "ram:RequestedResourceType" : [
        "glue:Table",
        "glue:Database",
        "glue:Catalog"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare",
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:ResourceShareName" : [
        "LakeFormation*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceSharePermission"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:PermissionArn" : [
        "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
      ]
    }
  }
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue>DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin é uma [política AWS gerenciada](#) que: Concede acesso administrativo ao AWS Lake Formation e serviços relacionados, como o AWS Glue, para gerenciar lagos de dados



## A utilização desta política

Você pode vincular a `AWSLakeFormationDataAdmin` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de agosto de 2019, 17:33 UTC
- Horário editado: 16 de dezembro de 2019, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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:GetWorkflow",
    "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" : "*"
},
{
  "Effect" : "Deny",
  "Action" : [
    "lakeformation:PutDataLakeSettings"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSLambda\_FullAccess

AWSLambda\_FullAccess é uma [política gerenciada AWS](#) que: concede acesso total ao serviço AWS Lambda, aos recursos do console AWS Lambda e a outros serviços relacionados do AWS.

## A utilização desta política

Você pode vincular a AWSLambda\_FullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de novembro de 2020, 21:14 UTC
- Horário editado: 17 de novembro de 2020, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
```

```

    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "lambda:*",
    "logs:DescribeLogGroups",
    "states:DescribeStateMachine",
    "states:ListStateMachines",
    "tag:GetResources",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "lambda.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:FilterLogEvents"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambda\_ReadOnlyAccess

AWSLambda\_ReadOnlyAccess é uma [política gerenciada da AWS](#) que: concede acesso somente leitura ao serviço AWS Lambda, aos recursos do console AWS Lambda e a outros serviços relacionados do AWS.

### A utilização desta política

Você pode vincular a AWSLambda\_ReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de novembro de 2020, 21:10 UTC
- Horário editado: 27 de julho de 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "kms:ListAliases",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "logs:DescribeLogGroups",
    "lambda:Get*",
    "lambda:List*",
    "states:DescribeStateMachine",
    "states:ListStateMachines",
    "tag:GetResources",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:FilterLogEvents",
    "logs:StartQuery",
    "logs:StopQuery",
    "logs:DescribeQueries",
    "logs:GetLogGroupFields",
    "logs:GetLogRecord",
    "logs:GetQueryResults"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaBasicExecutionRole

AWSLambdaBasicExecutionRole é uma [política AWS gerenciada](#) que: Fornece permissões de gravação para o CloudWatch Logs.

### A utilização desta política

Você pode vincular a AWSLambdaBasicExecutionRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de abril de 2015, 15:03 UTC
- Horário editado: 09 de abril de 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaDynamoDBExecutionRole

AWSLambdaDynamoDBExecutionRole é uma [política AWS gerenciada](#) que: fornece acesso de lista e leitura aos streams do DynamoDB e permissões de gravação nos registros do CloudWatch.

### A utilização desta política

Você pode vincular a AWSLambdaDynamoDBExecutionRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de abril de 2015, 15:09 UTC
- Horário editado: 09 de abril de 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess é uma [política AWS gerenciada](#) que: fornece permissões mínimas para uma função Lambda gerenciar ENIs (criar, descrever, excluir) usadas por uma função Lambda habilitada para VPC.

## A utilização desta política

Você pode vincular a AWSLambdaENIManagementAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de dezembro de 2016, 00:37 UTC
- Horário editado: 01 de outubro de 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaExecute

AWSLambdaExecute é uma [política AWS gerenciada](#) que: fornece Put, Get acesso ao S3 e acesso total ao CloudWatch Logs.

### A utilização desta política

Você pode vincular a AWSLambdaExecute aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaFullAccess

AWSLambdaFullAccess é uma [política gerenciada da AWS](#) que: Essa política está em um caminho de suspensão de uso. Consulte a documentação para obter orientação: <https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>. Fornece acesso total ao Lambda, S3, DynamoDB, CloudWatch Metrics and Logs.

## A utilização desta política

Você pode vincular a `AWSLambdaFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 27 de novembro de 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
    "events:*",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:PassRole",
    "iot:AttachPrincipalPolicy",
    "iot:AttachThingPrincipal",
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy",
    "iot:CreateThing",
    "iot:CreateTopicRule",
    "iot:DescribeEndpoint",
    "iot:GetTopicRule",
    "iot:ListPolicies",
    "iot:ListThings",
    "iot:ListTopicRules",
    "iot:ReplaceTopicRule",
    "kinesis:DescribeStream",
    "kinesis:ListStreams",
    "kinesis:PutRecord",
    "kms:ListAliases",
    "lambda:*",
    "logs:*",
    "s3:*",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTopics",
    "sns:Publish",
    "sns:Subscribe",
    "sns:Unsubscribe",
    "sqs:ListQueues",
    "sqs:SendMessage",
    "tag:GetResources",
    "xray:PutTelemetryRecords",
    "xray:PutTraceSegments"
  ],
  "Resource" : "*"
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaInvocation-DynamoDB

AWSLambdaInvocation-DynamoDB é uma [política AWS gerenciada](#) que: Fornece acesso de leitura ao DynamoDB Streams.

### A utilização desta política

Você pode vincular a AWSLambdaInvocation-DynamoDB aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 06 de fevereiro de 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:DescribeStream",
      "dynamodb:GetRecords",
      "dynamodb:GetShardIterator",
      "dynamodb:ListStreams"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaKinesisExecutionRole

AWSLambdaKinesisExecutionRole é uma [política AWS gerenciada](#) que: fornece acesso de lista e leitura aos streams do Kinesis e permissões de gravação nos logs do CloudWatch.

## A utilização desta política

Você pode vincular a AWSLambdaKinesisExecutionRole aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de abril de 2015, 15:14 UTC
- Horário editado: 19 de novembro de 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaMSKExecutionRole

AWSLambdaMSKExecutionRole é uma [política AWS gerenciada](#) que: fornece as permissões necessárias para acessar o MSK Cluster em uma VPC, gerenciar ENIs (criar, descrever, excluir) na VPC e gravar permissões no CloudWatch Logs.

### A utilização desta política

Você pode vincular a AWSLambdaMSKExecutionRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de agosto de 2020, 17:35 UTC
- Horário editado: 02 de agosto de 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "kafka:DescribeCluster",
      "kafka:DescribeClusterV2",
      "kafka:GetBootstrapBrokers",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeVpcs",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaReplicator

AWSLambdaReplicator é uma [política AWS gerenciada](#) que: Concede ao Lambda Replicator as permissões necessárias para replicar funções em todas as regiões

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de maio de 2017, 17:53 UTC
- Horário editado: 08 de dezembro de 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ],
    "Condition" : {
      "StringLikeIfExists" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CloudFrontListDistributions",
    "Effect" : "Allow",
    "Action" : [
      "cloudfront:ListDistributionsByLambdaFunction"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaRole

AWSLambdaRole é uma [política AWS gerenciada que: Política](#) padrão para a função de serviço AWS Lambda.

## A utilização desta política

Você pode vincular a AWSLambdaRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC

- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSLambdaSQSQueueExecutionRole

AWSLambdaSQSQueueExecutionRole é uma [política AWS gerenciada](#) que: fornece acesso a mensagens de recebimento, exclusão de mensagens e atributos de leitura às filas do SQS e permissões de gravação nos logs do CloudWatch.

## A utilização desta política

Você pode vincular a AWSLambdaSQSQueueExecutionRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de junho de 2018, 21:50 UTC
- Horário editado: 14 de junho de 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole é uma [política AWS gerenciada](#) que: fornece permissões mínimas para que uma função Lambda seja executada ao acessar um recurso em uma VPC — crie, descreva, exclua interfaces de rede e grave permissões em registros. CloudWatch

### Utilização desta política

Você pode vincular a AWSLambdaVPCAccessExecutionRole aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 11 de fevereiro de 2016, 23:15 UTC
- Horário editado: 05 de janeiro de 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLicenseManagerConsumptionPolicy

`AWSLicenseManagerConsumptionPolicy` é uma [política AWS gerenciada](#) que: Fornece permissões para permitir o acesso às ações da API AWS License Manager necessárias para consumir licenças às quais o usuário tem direitos.

## A utilização desta política

Você pode vincular a `AWSLicenseManagerConsumptionPolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de agosto de 2021, 23:18 UTC
- Horário editado: 11 de agosto de 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS License Manager Linux Subscriptions Service gere recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de dezembro de 2022, 18:54 UTC
- Horário editado: 20 de dezembro de 2022, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy é uma [política AWS gerenciada que: Política](#) de função da conta principal do serviço AWS License Manager

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2018, 19:03 UTC
- Horário editado: 31 de maio de 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",

```

```
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3::aws-license-manager-service-*"
  ]
},
{
  "Sid" : "S3ObjectPermissions1",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:PutObject",
    "s3:GetObject",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : [
    "arn:aws:s3::aws-license-manager-service-*"
  ]
},
{
  "Sid" : "S3ObjectPermissions2",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3::aws-license-manager-service-*/resource_sync/*"
  ]
},
{
  "Sid" : "AthenaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution"
  ],
  "Resource" : [
    "*"
  ]
},
{
```

```
"Sid" : "GluePermissions",
"Effect" : "Allow",
"Action" : [
  "glue:GetTable",
  "glue:GetPartition",
  "glue:GetPartitions"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "OrganizationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:DescribeAccount",
    "organizations:ListChildren",
    "organizations:ListParents",
    "organizations:ListAccountsForParent",
    "organizations:ListRoots",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "RAMPermissions1",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShares",
    "ram:GetResourceShareAssociations",
    "ram:TagResource"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "RAMPermissions2",
  "Effect" : "Allow",
  "Action" : [
```

```
    "ram:CreateResourceShare"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/Service" : "LicenseManager"
    }
  }
},
{
  "Sid" : "RAMPermissions3",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare",
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/Service" : "LicenseManager"
    }
  }
},
{
  "Sid" : "IAMGetRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "IAMPassRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
```



```

    ],
    "Resource" : [
      "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "cloudformation.amazonaws.com",
          "glue.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "CloudformationPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:UpdateStack",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : [
      "arn:aws:cloudformation::*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
    ]
  },
  {
    "Sid" : "GlueUpdatePermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateTable",
      "glue:UpdateTable",
      "glue>DeleteTable",
      "glue:UpdateJob",
      "glue:UpdateCrawler"
    ],
    "Resource" : [
      "arn:aws:glue::*:catalog",
      "arn:aws:glue::*:crawler/LicenseManagerResourceSynDataCrawler",
      "arn:aws:glue::*:job/LicenseManagerResourceSynDataProcessJob",
      "arn:aws:glue::*:table/license_manager_resource_inventory_db/*",
      "arn:aws:glue::*:table/license_manager_resource_sync/*",
      "arn:aws:glue::*:database/license_manager_resource_inventory_db",

```

```
    "arn:aws:glue:*:*:database/license_manager_resource_sync"
  ],
},
{
  "Sid" : "RGPermissions",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:PutGroupPolicy"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "ram.amazonaws.com"
      ]
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLicenseManagerMemberAccountRolePolicy

AWSLicenseManagerMemberAccountRolePolicy é uma [política AWS gerenciada que: Política de função da conta do membro do serviço do AWS License Manager](#)

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 26 de novembro de 2018, 19:04 UTC
- Horário editado: 15 de novembro de 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm>DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ]
    }
  ]
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "RAMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ram:AcceptResourceShareInvitation",
      "ram:GetResourceShareInvitations"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy é uma [política AWS gerenciada](#) que: política de função padrão do serviço AWS License Manager

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2018, 19:02 UTC
- Horário editado: 30 de julho de 2021, 01:43 UTC

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

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn::*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3BucketPermissions1",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-license-manager-service-*"
    ]
  },
  {
    "Sid" : "S3BucketPermissions2",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "S3ObjectPermissions",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-license-manager-service-*"
    ]
  },
  {
    "Sid" : "SNSAccountPermissions",
    "Effect" : "Allow",
    "Action" : [
      "sns:Publish"
    ],
    "Resource" : [
```

```
    "arn:aws:sns:*:*:aws-license-manager-service-*"
  ],
},
{
  "Sid" : "SNSTopicPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2Permissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeImages",
    "ec2:DescribeHosts"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "SSMPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListInventoryEntries",
    "ssm:GetInventory",
    "ssm:CreateAssociation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "OrganizationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganization",
    "organizations:ListDelegatedAdministrators"
  ]
}
```

```
    ],
    "Resource" : [
        "*"
    ]
  },
  {
    "Sid" : "LicenseManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
    ],
    "Resource" : [
        "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS License Manager User Subscriptions Service gerencie recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.



## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de julho de 2022, 01:17 UTC
- Horário editado: 21 de novembro de 2022, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "EC2ReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2WritePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:CreateTags"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:productCode" : [
          "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"
    }
  }
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSM2ServicePolicy

AWSM2ServicePolicy é uma [política AWS gerenciada](#) que: Permite que a AWS M2 gere recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de junho de 2022, 20:26 UTC
- Horário editado: 07 de junho de 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "fsx:DescribeFileSystems"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : [
        "AWS/M2"
      ]
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSManagedServices\_ContactsServiceRolePolicy

AWSManagedServices\_ContactsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Managed Services leia os valores das tags nos AWS recursos

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 23 de março de 2023, 17:07 UTC
- Horário editado: 23 de março de 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

```
}  
 ]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSManagedServices\_DetectiveControlsConfig\_ServiceRolePolicy

AWSManagedServices\_DetectiveControlsConfig\_ServiceRolePolicy é uma [política AWS gerenciada](#) que: AWS Managed Services - política para gerenciar a infraestrutura de controles de detetives

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de dezembro de 2022, 23:11 UTC
- Horário editado: 19 de dezembro de 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*:config-rule/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3>DeleteBucket",

```



```
    "s3:DeleteBucketPolicy",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:GetBucketAcl",
    "s3:PutObject",
    "s3:PutBucketAcl",
    "s3:PutBucketLogging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutEncryptionConfiguration"
  ],
  "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSManagedServices\_EventsServiceRolePolicy

AWSManagedServices\_EventsServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de AWS Managed Services para habilitar o recurso de processador de eventos do AMS.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de fevereiro de 2023, 18:41 UTC

- Horário editado: 07 de fevereiro de 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSManagedServicesDeploymentToolkitPolicy

AWSManagedServicesDeploymentToolkitPolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Managed Services gerencie o kit de ferramentas de implantação em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de junho de 2022, 18:33 UTC
- Horário editado: 10 de maio de 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

```
"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*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr>DeleteLifecyclePolicy",
    "ecr>DeleteRepository",
    "ecr>DeleteRepositoryPolicy",
    "ecr:DescribeRepositories",
    "ecr:GetLifecyclePolicy",
    "ecr:ListTagsForResource",
    "ecr:PutImageTagMutability",
    "ecr:PutLifecyclePolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion é uma [política AWS gerenciada](#) que: Permite AWS Marketplace copiar suas imagens de máquina da Amazon (AMIs) para listá-las no AWS Marketplace

### A utilização desta política

Você pode vincular a AWSMarketplaceAmiIngestion aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de setembro de 2020, 20:55 UTC
- Horário editado: 25 de setembro de 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
```

```
  },
  {
    "Action" : [
      "ec2:DescribeImageAttribute",
      "ec2:DescribeImages",
      "ec2:DescribeSnapshotAttribute",
      "ec2:ModifyImageAttribute"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy é uma [política gerenciada pela AWS](#) que: permite AWS Marketplace criar e gerenciar parâmetros de implantação do vendedor para os produtos que você assina no AWS Marketplace.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de novembro de 2023, 23:34 UTC

- Hora da edição: 15 de novembro de 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "TagMarketplaceDeploymentSecrets",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/expirationDate" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "expirationDate"
        ]
      },
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceFullAccess

AWSMarketplaceFullAccess é uma [política gerenciada da AWS](#) que: Fornece a capacidade de assinar e cancelar a assinatura do software AWS Marketplace, permite que os usuários gerenciem instâncias de software do Marketplace a partir da página "Seu software" do Marketplace e fornece acesso administrativo ao EC2.

## A utilização desta política

Você pode vincular a `AWSMarketplaceFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de fevereiro de 2015, 17:21 UTC
- Horário editado: 04 de março de 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2>DeleteSecurityGroup",
```

```
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcs",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DeregisterImage",
    "ec2:DescribeSnapshots",
    "ec2>DeleteSnapshot",
    "ec2>CreateImage",
    "ec2:DescribeInstanceStatus",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:DescribeDocument",
    "sns:ListTopics",
    "sns:GetTopicAttributes",
    "sns:CreateTopic",
    "iam:GetRole",
    "iam:GetInstanceProfile",
    "iam:ListRoles",
    "iam:ListInstanceProfiles"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "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/*"
    ]
  }
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceGetEntitlements

AWSMarketplaceGetEntitlements é uma [política AWS gerenciada](#) que: Fornece acesso de leitura aos AWS Marketplace direitos

## A utilização desta política

Você pode vincular a `AWSMarketplaceGetEntitlements` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de março de 2017, 19:37 UTC
- Horário editado: 27 de março de 2017, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao recurso de criação de imagem AWS Marketplace privada. Além de criar imagens privadas, ele também fornece permissões para adicionar tags às imagens, iniciar e encerrar instâncias ec2.

### A utilização desta política

Você pode vincular a AWSMarketplaceImageBuildFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 31 de julho de 2018, 23:29 UTC
- Horário editado: 04 de março de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "aws-marketplace:StartBuild",
    "aws-marketplace:DescribeBuilds"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:TerminateInstances",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam::*:role/*Automation*",
    "arn:aws:iam::*:role/*Instance*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:DescribeDocument",
    "ec2:DeregisterImage",
    "ec2:CopyImage",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2>DeleteSnapshot",
    "ec2:CreateImage",
```



```
    "ec2:RunInstances",
    "ec2:DescribeInstanceStatus",
    "sns:GetTopicAttributes",
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3::*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2::*:image/*",
    "arn:aws:ec2::*:instance/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns::*:*image-build*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
```

```
    "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
    "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
    "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
    "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
    "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
    "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
    "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ],
      "iam:AssociatedResourceARN" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
```

```
    "StringLike" : {
      "aws:RequestTag/marketplace-image-build:build-id" : "*"
    },
    "StringNotEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceLicenseManagementServiceRolePolicy

AWSMarketplaceLicenseManagementServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo AWS Marketplace para gerenciamento de licenças.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de dezembro de 2020, 08:33 UTC
- Horário editado: 03 de dezembro de 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager>DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions é uma [política AWS gerenciada](#) que: Fornece a capacidade de assinar e cancelar a AWS Marketplace assinatura de software

## A utilização desta política

Você pode vincular a AWSMarketplaceManageSubscriptions aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 19 de janeiro de 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceMeteringFullAccess

AWSMarketplaceMeteringFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à AWS Marketplace medição.

### A utilização desta política

Você pode vincular a AWSMarketplaceMeteringFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de março de 2016, 22:39 UTC

- Horário editado: 17 de março de 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSMarketplaceMeteringRegisterUsage

AWSMarketplaceMeteringRegisterUsage é uma [política AWS gerenciada](#) que: fornece permissões para registrar um recurso e monitorar o uso por meio do AWS Marketplace Metering Service.

## A utilização desta política

Você pode vincular a AWSMarketplaceMeteringRegisterUsage aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de novembro de 2019, 01:17 UTC
- Horário editado: 21 de novembro de 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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



}

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceProcurementSystemAdminFullAccess

AWSMarketplaceProcurementSystemAdminFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total a todas as ações administrativas para uma integração do AWS Marketplace eProcurement.

### A utilização desta política

Você pode vincular a AWSMarketplaceProcurementSystemAdminFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de junho de 2019, 13:07 UTC
- Horário editado: 25 de junho de 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplacePurchaseOrdersServiceRolePolicy

AWSMarketplacePurchaseOrdersServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso de AWS Marketplace serviços ao gerenciamento de pedidos de compra.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de outubro de 2021, 15:12 UTC
- Horário editado: 27 de outubro de 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSMarketplaceRead-only

AWSSMarketplaceRead-only é uma [política AWS gerenciada](#) que: Fornece a capacidade de revisar AWS Marketplace assinaturas

### A utilização desta política

Você pode vincular a AWSSMarketplaceRead-only aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 19 de janeiro de 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSMarketplaceRead-only`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceResaleAuthorizationServiceRolePolicy

AWSMarketplaceResaleAuthorizationServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela AWS Marketplace para autorização de revenda.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de março de 2024, 18:47 UTC
- Horário editado: 05 de março de 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

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

```

    "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare"
    ],
    "Resource" : [
      "arn:aws:ram:*:*:*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ram:RequestedResourceType" : "aws-marketplace:Entity"
      },
      "ArnLike" : {
        "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      },
      "Null" : {
        "ram:Principal" : "true"
      }
    }
  },
  {
    "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceShare"
    ],
    "Resource" : [
      "arn:aws:ram:*:*:*"
    ],
    "Condition" : {
      "Null" : {
        "ram:Principal" : "false"
      },
      "StringEquals" : {
        "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
      }
    }
  },
  {
    "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
    "Effect" : "Allow",
    "Action" : [
      "ram:AcceptResourceShareInvitation"
    ]
  }
}

```

```

    ],
    "Resource" : [
        "arn:aws:ram:*:*:*"
    ],
    "Condition" : {
        "StringEquals" : {
            "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
    }
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
    "Effect" : "Allow",
    "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
    ],
    "Resource" : [
        "arn:aws:ram:*:*:*"
    ]
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:CalledVia" : [
                "ram.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
    "Effect" : "Allow",
    "Action" : [
        "aws-marketplace:DescribeEntity"
    ],
    "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
}

```



```
}  
]  
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSMarketplaceSellerFullAccess

AWSMarketplaceSellerFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total a todas as operações do vendedor no AWS Marketplace e em outros AWS serviços, como gerenciamento de AMI.

### Utilização desta política

Você pode vincular a AWSMarketplaceSellerFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 02 de julho de 2019, 20:40 UTC
- Horário editado: 15 de março de 2024, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSMarketplaceSellerProductsFullAccess

AWSMarketplaceSellerProductsFullAccess é uma [política AWS gerenciada](#) que: Fornece aos vendedores acesso total à página AWS Marketplace de produtos de gerenciamento e a outros AWS serviços, como gerenciamento de AMI.

### A utilização desta política

Você pode vincular a AWSMarketplaceSellerProductsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de julho de 2019, 21:06 UTC
- Horário editado: 18 de julho de 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace: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/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMarketplaceSellerProductsReadOnly

AWSMarketplaceSellerProductsReadOnly é uma [política AWS gerenciada](#) que: Fornece aos vendedores acesso somente para leitura à página de produtos AWS Marketplace de gerenciamento.

### A utilização desta política

Você pode vincular a AWSMarketplaceSellerProductsReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de julho de 2019, 21:40 UTC
- Horário editado: 19 de novembro de 2022, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy é uma [política AWS gerenciada](#) que: A política padrão que permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo MediaConnect.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de abril de 2023, 22:11 UTC
- Horário editado: 03 de abril de 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs>DeleteService",
        "ecs>CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs>DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
```

```
    "ecs:StopTask",
    "ecs:DescribeTasks",
    "ecs:DescribeContainerInstances",
    "ecs:UpdateContainerInstancesState"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateCluster",
    "ecs:UpdateClusterSettings",
    "ecs:ListAttributes",
    "ecs:DescribeClusters",
    "ecs:DeregisterContainerInstance",
    "ecs:ListContainerInstances"
  ],
  "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso aos AWS recursos usados ou gerenciados pelo MediaTailor

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de setembro de 2021, 22:27 UTC
- Horário editado: 17 de setembro de 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubDiscoveryAccess

AWSMigrationHubDiscoveryAccess é uma [política AWS gerenciada que: A política](#) permite que o AWSMigrationHubService chame o AWSApplicationDiscoveryService em nome do cliente.

### A utilização desta política

Você pode vincular a AWSMigrationHubDiscoveryAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de agosto de 2017, 13:30 UTC
- Horário editado: 06 de agosto de 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstanceAttribute"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubDMSAccess

AWSMigrationHubDMSAccess é uma [política AWS gerenciada que: Política](#) para que o Database Migration Service assuma uma função na conta do cliente para ligar para o Migration Hub

### A utilização desta política

Você pode vincular a AWSMigrationHubDMSAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de agosto de 2017, 14:00 UTC
- Horário editado: 07 de outubro de 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh>ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh>ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
    }
  ]
}
```



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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubFullAccess

AWSMigrationHubFullAccess é uma [política AWS gerenciada](#) que: Política gerenciada para fornecer ao cliente acesso ao Serviço Migration Hub

### A utilização desta política

Você pode vincular a AWSMigrationHubFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de agosto de 2017, 14:02 UTC
- Horário editado: 19 de junho de 2019, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {

```

```
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "migrationhub.amazonaws.com",
          "dmsintegration.migrationhub.amazonaws.com",
          "smsintegration.migrationhub.amazonaws.com"
        ]
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubOrchestratorConsoleFullAccess

A `AWSMigrationHubOrchestratorConsoleFullAccess` é uma [política gerenciada pela AWS](#) que: fornece acesso limitado ao AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service e o AWS Secrets Manager. Esta política também concede acesso total ao serviço do AWS Migration Hub Orchestrator.

### Utilização desta política

Você pode vincular a `AWSMigrationHubOrchestratorConsoleFullAccess` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS

- Horário de criação: 20 de abril de 2022, 02:26 UTC
- Horário editado: 05 de dezembro de 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy é uma [política AWS gerenciada](#) que: Essa política precisa ser anexada à instância migrada para SAP e MGN para que nosso serviço orchestre instâncias baixando scripts do S3 e busque valores secretos dentro da instância EC2.

### A utilização desta política

Você pode vincular a AWSMigrationHubOrchestratorInstanceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de abril de 2022, 02:43 UTC

- Horário editado: 20 de abril de 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)



- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubOrchestratorPlugin

AWSMigrationHubOrchestratorPlugin é uma [política AWS gerenciada](#) que: Fornece acesso limitado às ações relacionadas ao Amazon Simple Storage Service, AWS Secrets Manager e plug-in para o AWS Migration Hub Orchestrator.

### A utilização desta política

Você pode vincular a AWSMigrationHubOrchestratorPlugin aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de abril de 2022, 02:25 UTC
- Horário editado: 20 de abril de 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "s3:CreateBucket",
  "s3:PutObject",
  "s3:GetObject",
  "s3:GetBucketAcl"
],
"Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "execute-api:Invoke",
    "execute-api:ManageConnections"
  ],
  "Resource" : [
    "arn:aws:execute-api:*:*:*/*prod/*/*put-log-data",
    "arn:aws:execute-api:*:*:*/*prod/*/*put-metric-data"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "migrationhub-orchestrator:RegisterPlugin",
    "migrationhub-orchestrator:GetMessage",
    "migrationhub-orchestrator:SendMessage"
  ],
  "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
}
]
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubOrchestratorServiceRolePolicy

A `AWSMigrationHubOrchestratorServiceRolePolicy` é uma [política gerenciada pela AWS](#) que: Fornece as permissões necessárias para que o Migration Hub Orchestrator migre e modernize seus workloads on-premises

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de abril de 2022, 02:24 UTC
- Horário editado: 04 de março de 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ec2LaunchTemplates",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "getHomeRegion",
    "Action" : [
      "mgh:GetHomeRegion"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Sid" : "SSMcommand",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:GetCommandInvocation",
      "ssm:CancelCommand"
    ],
    "Resource" : [
      "arn:aws:ssm:*::document/AWS-RunRemoteScript",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:s3:::aws-migrationhub-orchestrator-*",
      "arn:aws:s3:::migrationhub-orchestrator-*"
    ]
  },
  {
    "Sid" : "SSM",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation",
```

```
    "ssm:GetCommandInvocation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "s3GetObject",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::migrationhub-orchestrator-*",
    "arn:aws:s3:::migrationhub-orchestrator-*/*"
  ]
},
{
  "Sid" : "EventBridge",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:DescribeRule",
    "events>DeleteRule",
    "events:PutRule",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
},
{
  "Sid" : "MGN",
  "Effect" : "Allow",
  "Action" : [
    "mgn:GetReplicationConfiguration",
    "mgn:GetLaunchConfiguration",
    "mgn:StartCutover",
    "mgn:FinalizeCutover",
    "mgn:StartTest",
    "mgn:UpdateReplicationConfiguration",
    "mgn:DescribeSourceServers",
    "mgn:MarkAsArchived",
    "mgn:ChangeServerLifeCycleState"
  ],
  "Resource" : "*"
}
```

```
  },
  {
    "Sid" : "ec2DescribeImportImage",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImportImageTasks"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "s3ListBucket",
    "Effect" : "Allow",
    "Action" : "s3:ListBucket",
    "Resource" : "arn:aws:s3:::*",
    "Condition" : {
      "StringLike" : {
        "s3:prefix" : "migrationhub-orchestrator-vmie-*"
      }
    }
  }
]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total aos AWS Migration Hub Refactor Spaces e a outros serviços AWS relacionados, exceto aos grupos de segurança AWS Transit Gateway e EC2, não necessários ao usar ambientes sem uma ponte de rede. Essa política também exclui as permissões necessárias para o AWS Lambda AWS e o Resource Access Manager, pois elas podem ser definidas com base em tags.

## A utilização desta política

Você pode vincular a `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de abril de 2023, 20:09 UTC
- Horário editado: 20 de julho de 2023, 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
```



```

    "ec2:DescribeTags",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeInternetGateways"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpointServiceConfiguration"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteTags"
  ],
  "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:AddTags",
    "elasticloadbalancing:CreateLoadBalancer"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
  "Condition" : {

```

```

    "Null" : {
      "aws:RequestTag/refactor-spaces:application-id" : "false"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
  },
  {
    "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" : "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:AddTags",
    "elasticloadbalancing>CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "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"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : [
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",

```

```
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy é uma [política AWS gerenciada](#) que: Use na função de serviço do IAM passada para o documento de automação SSM AWSRefatorSpaces-CreateResources para conceder as permissões necessárias para executar a automação. A política concede acesso de leitura/gravação às tags do EC2 para acompanhar o progresso da automação. Quando a ponte de rede do ambiente Refactor Spaces é ativada, a automação também adiciona o grupo de segurança do ambiente à instância do EC2 para permitir o tráfego de outros serviços do Refactor Spaces no ambiente. A política também concede acesso aos parâmetros SSM das ações pós-lançamento do Serviço de Migração de Aplicativos.

## A utilização desta política

Você pode vincular a `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 10 de agosto de 2023, 15:08 UTC
- Horário editado: 10 de agosto de 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],

```

```

    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyInstanceAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags",
      "ec2>DeleteTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ssm:GetParameters",
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubRefactorSpacesFullAccess

AWSMigrationHubRefactorSpacesFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total ao AWS MigrationHub Refactor Spaces, aos recursos do console do AWS MigrationHub Refactor Spaces e a outros serviços relacionados, AWS exceto as permissões necessárias para o Lambda AWS e o Resource AWS Access Manager, pois eles podem ser definidos com base em tags.

### A utilização desta política

Você pode vincular a AWSMigrationHubRefactorSpacesFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2021, 07:12 UTC
- Horário editado: 19 de julho de 2023, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```

    "Sid" : "RefactorSpaces",
    "Effect" : "Allow",
    "Action" : [
      "refactor-spaces:*"
    ],
    "Resource" : "*"
  },
  {
    "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" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTransitGateway",
      "ec2:CreateSecurityGroup",
      "ec2:CreateTransitGatewayVpcAttachment"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:environment-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTransitGateway",
      "ec2:CreateSecurityGroup",
      "ec2:CreateTransitGatewayVpcAttachment"
    ]
  }

```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:environment-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpointServiceConfiguration"
    ],
    "Resource" : "*"
  },
  {
    "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"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  }
},
```

```

{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateLoadBalancer"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeListeners"
  ],
  "Resource" : "*"
},
{
  "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" : "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:AddTags",
      "elasticloadbalancing>CreateTargetGroup"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  }
}

```

```
    }
  }
},
{
  "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"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : [
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
```

```
    "Action" : [
      "cloudformation:CreateStack"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSMigrationHubRefactorSpacesServiceRolePolicy

AWSMigrationHubRefactorSpacesServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS recursos gerenciados ou usados pelo AWS Migration Hub Refactor Spaces.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2021, 06:50 UTC
- Horário editado: 20 de julho de 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
```

```

    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetGroups",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTransitGatewayVpcAttachment",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2>DeleteTags",
    "ram>DeleteResourceShare",
    "ram:AssociateResourceShare",
    "ram:DisassociateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2>DeleteVpcEndpointServiceConfigurations",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets",

```



```

    "elasticloadbalancing:CreateLoadBalancerListeners",
    "elasticloadbalancing:CreateListener",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/refactor-spaces:route-id" : [
        "*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "apigateway:PUT",
    "apigateway:POST",
    "apigateway:GET",
    "apigateway:PATCH",
    "apigateway:DELETE"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/vpclinks/*",
    "arn:aws:apigateway:*::/tags",
    "arn:aws:apigateway:*::/tags/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "apigateway:GET",
  "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
},
{
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteLoadBalancer",

```

```

    "Resource" : "arn::*:elasticloadbalancing::*:loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn::*:elasticloadbalancing::*:loadbalancer/net/refactor-spaces-nlb-*",
      "arn::*:elasticloadbalancing::*:listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteListener",
    "Resource" : "arn::*:elasticloadbalancing::*:listener/net/refactor-spaces-nlb-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing>DeleteTargetGroup",
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn::*:elasticloadbalancing::*:targetgroup/refactor-spaces-tg-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DeregisterTargets"
    ],
    "Resource" : "arn::*:elasticloadbalancing::*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:route-id" : "false"
      }
    }
  }
},

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateTargetGroup"
  ],
  "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess é uma [política AWS gerenciada que: Política](#) para que o Serviço de Migração de Servidores assuma uma função na conta do cliente para ligar para o Migration Hub

## A utilização desta política

Você pode vincular a AWSMigrationHubSMSAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de agosto de 2017, 13:57 UTC
- Horário editado: 07 de outubro de 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh>ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh>ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh>ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
    }
  ]
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubStrategyCollector

AWSMigrationHubStrategyCollector é uma [política gerenciada pela AWS](#) que: concede permissões para a comunicação com o serviço do AWS Migration Hub Strategy Recommendations, acesso de leitura/gravação aos buckets do S3 relacionados ao serviço, acesso ao Amazon API Gateway para fazer upload de registros e métricas, acesso ao AWS, AWS Secrets Manager para buscar credenciais e quaisquer serviços relacionados.

### Utilização desta política

Você pode vincular a AWSMigrationHubStrategyCollector aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 19 de outubro de 2021, 20:15 UTC
- Horário editado: 05 de fevereiro de 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "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}"
        }
      }
    }
  ],
  {
```



```
}  
  }  
    }  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMigrationHubStrategyConsoleFullAccess

AWSMigrationHubStrategyConsoleFullAccess é uma [política AWS gerenciada](#) que: Concede acesso total ao serviço de Recomendações de Estratégia do AWS Migration Hub e acesso aos AWS serviços relacionados por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a AWSMigrationHubStrategyConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 19 de outubro de 2021, 20:13 UTC
- Horário editado: 09 de novembro de 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

### Versão da política

Versão da política: v2 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "discovery:GetDiscoverySummary",
    "discovery:DescribeTags",
    "discovery:DescribeConfigurations",
    "discovery:ListConfigurations"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSMigrationHubStrategyServiceRolePolicy

AWSMigrationHubStrategyServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso aos AWS recursos usados ou gerenciados pelo serviço AWS Migration Hub Strategy Recommendations.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de outubro de 2021, 20:02 UTC
- Horário editado: 19 de outubro de 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
```

```
    "mgh:GetHomeRegion"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Sid" : "permissionsForS3",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl"
  ],
  "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMobileHub\_FullAccess

AWSMobileHub\_FullAccess é uma [política AWS gerenciada](#) que: Esta política pode ser anexada a qualquer usuário, função ou grupo, a fim de conceder aos usuários permissão para criar, excluir e modificar projetos (e seus AWS recursos associados) no AWS Mobile Hub. Isso também inclui permissões para gerar e baixar amostras de código-fonte do aplicativo móvel para cada projeto do Mobile Hub.

## A utilização desta política

Você pode vincular a `AWSMobileHub_FullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de janeiro de 2016, 19:56 UTC
- Horário editado: 19 de dezembro de 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

## Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
```

```
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "iam:ListSAMLProviders",
    "lambda:ListFunctions",
    "sns:ListTopics",
    "lex:GetIntent",
    "lex:GetIntents",
    "lex:GetSlotType",
    "lex:GetSlotTypes",
    "lex:GetBot",
    "lex:GetBots",
    "lex:GetBotAlias",
    "lex:GetBotAliases",
    "mobilehub:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject"
  ],
  "Resource" : "arn:aws:s3::*-mobilehub-*/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3::*-mobilehub-*"
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMobileHub\_ReadOnly

AWSMobileHub\_ReadOnly é uma [política AWS gerenciada](#) que: Esta política pode ser anexada a qualquer usuário, função ou grupo, a fim de conceder aos usuários permissão para listar e visualizar projetos no AWS Mobile Hub. Isso também inclui permissões para gerar e baixar amostras de código-fonte do aplicativo móvel para cada projeto do Mobile Hub. Ele não permite que o usuário modifique nenhuma configuração para nenhum projeto do Mobile Hub.

### A utilização desta política

Você pode vincular a AWSMobileHub\_ReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 05 de janeiro de 2016, 19:55 UTC
- Horário editado: 23 de julho de 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
        "mobilehub:GetProjectSnapshot",
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
    }
  ]
}
```



```
    "Resource" : "arn:aws:s3::*/aws-my-sample-app*.zip"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSMSKReplicatorExecutionRole

AWSMSKReplicatorExecutionRole é uma [política AWS gerenciada](#) que: concede permissões ao Amazon MSK Replicator para replicar dados entre clusters MSK.

### Utilização desta política

Você pode vincular a AWSMSKReplicatorExecutionRole aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 06 de dezembro de 2023, 00:07 UTC
- Horário editado: 06 de dezembro de 2023, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration"
      ],
      "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/*/*"
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSNetworkFirewallServiceRolePolicy

AWSNetworkFirewallServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWSNetworkFirewall crie e gerencie os recursos necessários para seus firewalls.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de novembro de 2020, 17:17 UTC
- Horário editado: 30 de março de 2023, 17:19 UTC

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

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaLast" : "resource-groups.amazonaws.com"
      }
    },
  ],
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o NetworkManager acesse os recursos associados à sua rede principal

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de julho de 2022, 12:17 UTC
- Horário editado: 12 de julho de 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSNetworkManagerFullAccess

`AWSNetworkManagerFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon NetworkManager por meio do. AWS Management Console

### A utilização desta política

Você pode vincular a `AWSNetworkManagerFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 17:37 UTC
- Horário editado: 03 de dezembro de 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "networkmanager:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "networkmanager.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSNetworkManagerReadOnlyAccess

`AWSNetworkManagerReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon NetworkManager por meio do. AWS Management Console

## A utilização desta política

Você pode vincular a `AWSNetworkManagerReadOnlyAccess` aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de dezembro de 2019, 17:35 UTC
- Horário editado: 03 de dezembro de 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSNetworkManagerServiceRolePolicy

AWSNetworkManagerServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o NetworkManager acesse recursos associados às suas redes globais

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de dezembro de 2019, 14:03 UTC
- Horário editado: 27 de julho de 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Action" : [
  "directconnect:DescribeDirectConnectGateways",
  "directconnect:DescribeConnections",
  "directconnect:DescribeDirectConnectGatewayAttachments",
  "directconnect:DescribeLocations",
  "directconnect:DescribeVirtualInterfaces",
  "ec2:DescribeCustomerGateways",
  "ec2:DescribeTransitGatewayAttachments",
  "ec2:DescribeTransitGatewayRouteTables",
  "ec2:DescribeTransitGateways",
  "ec2:DescribeVpnConnections",
  "ec2:DescribeVpcs",
  "ec2:GetTransitGatewayRouteTableAssociations",
  "ec2:GetTransitGatewayRouteTablePropagations",
  "ec2:SearchTransitGatewayRoutes",
  "ec2:DescribeTransitGatewayPeeringAttachments",
  "ec2:DescribeTransitGatewayConnects",
  "ec2:DescribeTransitGatewayConnectPeers",
  "ec2:DescribeRegions",
  "organizations:DescribeAccount",
  "organizations:DescribeOrganization",
  "organizations:ListAccounts",
  "organizations:ListAWSServiceAccessForOrganization",
  "organizations:ListDelegatedAdministrators",
  "ec2:DescribeTransitGatewayRouteTableAnnouncements",
  "ec2:DescribeTransitGatewayPolicyTables",
  "ec2:GetTransitGatewayPolicyTableAssociations",
  "ec2:GetTransitGatewayPolicyTableEntries"
],
"Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSOpsWorks\_FullAccess

AWSOpsWorks\_FullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao AWS OpsWorks.

## A utilização desta política

Você pode vincular a AWSOpsWorks\_FullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de janeiro de 2021, 16:29 UTC
- Horário editado: 22 de janeiro de 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancers",
    "iam:GetRolePolicy",
    "iam:ListInstanceProfiles",
    "iam:ListRoles",
    "iam:ListUsers",
    "opsworks:*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "opsworks.amazonaws.com"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs é uma [política AWS gerenciada](#) que: Permite que as instâncias do OpsWorks com a integração do CWLogs habilitada enviem registros e criem os grupos de registros necessários

## A utilização desta política

Você pode vincular a `AWSOpsWorksCloudWatchLogs` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de março de 2017, 17:47 UTC
- Horário editado: 30 de março de 2017, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOpsWorksCMInstanceProfileRole

AWSOpsWorksCMInstanceProfileRole é uma [política AWS gerenciada](#) que: fornece acesso ao S3 para instâncias lançadas pelo OpsWorks CM.

### A utilização desta política

Você pode vincular a AWSOpsWorksCMInstanceProfileRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de novembro de 2016, 09:48 UTC
- Horário editado: 23 de abril de 2021, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "cloudformation:DescribeStackResource",
      "cloudformation:SignalResource"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ]
  },
  {
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:GetObject",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:ListMultipartUploadParts",
      "s3:PutObject"
    ],
    "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
    "Effect" : "Allow"
  },
  {
    "Action" : "acm:GetCertificate",
    "Resource" : "*",
    "Effect" : "Allow"
  },
  {
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
    "Effect" : "Allow"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOpsWorksCMServiceRole

AWSOpsWorksCMServiceRole é uma [política AWS gerenciada que: Política](#) de função de serviço a ser usada para criar servidores OpsWorks CM.

### A utilização desta política

Você pode vincular a AWSOpsWorksCMServiceRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de novembro de 2016, 09:49 UTC
- Horário editado: 23 de abril de 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
```

```
    "s3:DeleteObject",
    "s3:DeleteBucket",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutBucketPolicy",
    "s3:PutObject",
    "s3:GetBucketTagging",
    "s3:PutBucketTagging"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "tag:UntagResources",
    "tag:TagResources"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation",
    "ssm:ListCommandInvocations",
    "ssm:ListCommands"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
    }
  }
},
  "Action" : [
    "ssm:SendCommand"
  ]
}
```

```
]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:ssm:*::document/*",
    "arn:aws:s3:::aws-opsworks-cm-*"
  ],
  "Action" : [
    "ssm:SendCommand"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ],
  "Action" : [
    "ec2:AllocateAddress",
    "ec2:AssociateAddress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateImage",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSnapshot",
    "ec2:CreateTags",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteSnapshot",
    "ec2:DeregisterImage",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DisassociateAddress",
    "ec2:ReleaseAddress",
    "ec2:RunInstances",
    "ec2:StopInstances"
  ]
},
{
  "Effect" : "Allow",
```

```
"Resource" : [
  "*"
],
"Condition" : {
  "StringLike" : {
    "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
  }
},
"Action" : [
  "ec2:TerminateInstances",
  "ec2:RebootInstances"
],
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:opsworks-cm:*:*:server/*"
  ],
  "Action" : [
    "opsworks-cm:DeleteServer",
    "opsworks-cm:StartMaintenance"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
  ],
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:UpdateStack"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-opsworks-cm-*",
    "arn:aws:iam:*:*:role/service-role/aws-opsworks-cm-*"
  ],
  "Action" : [
```

```
    "iam:PassRole"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : "*",
  "Action" : [
    "acm:DeleteCertificate",
    "acm:ImportCertificate"
  ]
},
{
  "Effect" : "Allow",
  "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:UpdateSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:TagResource",
    "secretsmanager:UntagResource"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:DeleteTags",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:elastic-ip/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSOpsWorksInstanceRegistration

AWSOpsWorksInstanceRegistration é uma [política AWS gerenciada](#) que: fornece acesso para que uma instância do Amazon EC2 se registre em uma pilha do OpsWorksAWS.

## A utilização desta política

Você pode vincular a AWSOpsWorksInstanceRegistration aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de junho de 2016, 14:23 UTC
- Horário editado: 03 de junho de 2016, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    ]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOpsWorksRegisterCLI\_EC2

AWSOpsWorksRegisterCLI\_EC2 é uma [política AWS gerenciada que: Política](#) para permitir o registro de instâncias do EC2 por meio da CLI do OpsWorks

### A utilização desta política

Você pode vincular a AWSOpsWorksRegisterCLI\_EC2 aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 18 de junho de 2019, 15:56 UTC
- Horário editado: 18 de junho de 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSOpsWorksRegisterCLI\_OnPremises

AWSOpsWorksRegisterCLI\_OnPremises é uma [política gerenciada da AWS](#) que: Política para permitir o registro de instâncias on-premises por meio da CLI do OpsWorks

## A utilização desta política

Você pode vincular a AWSOpsWorksRegisterCLI\_OnPremises aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 18 de junho de 2019, 15:33 UTC
- Horário editado: 18 de junho de 2019, 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateGroup",
      "iam:AddUserToGroup"
    ],
    "Resource" : [
      "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateUser",
      "iam:CreateAccessKey"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:AttachUserPolicy"
    ],
    "Resource" : [
      "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
    ],
    "Condition" : {
      "ArnEquals" : {
```

```
    "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOrganizationsFullAccess

AWSOrganizationsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total às AWS Organizations.

### Utilização desta política

Você pode vincular a AWSOrganizationsFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de novembro de 2018, 20:31 UTC
- Horário editado: 06 de fevereiro de 2024, 17:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSOrganizationsReadOnlyAccess

`AWSOrganizationsReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura às Organizations AWS .

### Utilização desta política

Você pode vincular a `AWSOrganizationsReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de novembro de 2018, 20:32 UTC
- Horário editado: 06 de fevereiro de 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "AWSOrganizationsReadOnly",
    "Effect" : "Allow",
    "Action" : [
      "organizations:Describe*",
      "organizations:List*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSOrganizationsReadOnlyAccount",
    "Effect" : "Allow",
    "Action" : [
      "account:GetAlternateContact",
      "account:GetContactInformation",
      "account:ListRegions"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSOrganizationsServiceTrustPolicy

AWSOrganizationsServiceTrustPolicy é uma [política AWS gerenciada](#) que: Uma política que permite que AWS as Organizations compartilhem confiança com outras pessoas aprovadas Serviços da AWS com o objetivo de simplificar a configuração do cliente.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 10 de outubro de 2017, 23:04 UTC
- Horário editado: 01 de novembro de 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy é uma [política gerenciada da AWS](#) que: Essa política concede permissões que permitem que você instale um servidor Outpost em sua rede on-premise.

### A utilização desta política

Você pode vincular a AWSOutpostsAuthorizeServerPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de janeiro de 2023, 19:23 UTC
- Horário editado: 04 de janeiro de 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:StartConnection",
      "outposts:GetConnection"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSOutpostsServiceRolePolicy

AWSOutpostsServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de função vinculada ao serviço para permitir o acesso aos AWS recursos gerenciados pelo AWS Outposts

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de novembro de 2020, 22:55 UTC
- Horário editado: 09 de novembro de 2020, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaApplianceRolePolicy

AWSPanoramaApplianceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o software de AWS IoT em um dispositivo AWS Panorama faça upload de registros para o Amazon CloudWatch.

## A utilização desta política

Você pode vincular a `AWSPanoramaApplianceRolePolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de dezembro de 2020, 13:13 UTC
- Horário editado: 01 de dezembro de 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaApplianceServiceRolePolicy

AWSPanoramaApplianceServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que um dispositivo AWS Panorama faça upload de registros para o Amazon CloudWatch e obtenha objetos dos pontos de acesso do Amazon S3 criados para uso com o Panorama. AWS

### A utilização desta política

Você pode vincular a AWSPanoramaApplianceServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de outubro de 2021, 12:14 UTC
- Horário editado: 17 de janeiro de 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",

```

```
    "s3:ListBucket",
    "s3:GetObjectVersion"
  ],
  "Resource" : [
    "arn:aws:s3:::*-nodepackage-store-*",
    "arn:aws:s3:::*-application-payload-store-*",
    "arn:aws:s3:*:*:accesspoint/panorama*"
  ],
  "Condition" : {
    "StringLike" : {
      "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaFullAccess

AWSPanoramaFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Panorama

### A utilização desta política

Você pode vincular a AWSPanoramaFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2020, 13:12 UTC
- Horário editado: 12 de janeiro de 2022, 21:21 UTC

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

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "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"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSPanoramaGreengrassGroupRolePolicy

AWSPanoramaGreengrassGroupRolePolicy é uma [política AWS gerenciada](#) que: permite que uma função AWS Lambda em um dispositivo AWS Panorama gerencie recursos no Panorama, carregue registros e métricas no Amazon CloudWatch e gerencie objetos em buckets criados para uso com o Panorama.

## A utilização desta política

Você pode vincular a AWSPanoramaGreengrassGroupRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de dezembro de 2020, 13:10 UTC
- Horário editado: 06 de janeiro de 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",

```

```

        "s3:GetObject",
        "s3:PutObject"
    ],
    "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
    ]
},
{
    "Sid" : "PanoramaCloudWatchPutDashboard",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutDashboard",
    "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
    ]
},
{
    "Sid" : "PanoramaCloudWatchPutMetricData",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*"
},
{
    "Sid" : "PanoramaGreenGrassCloudWatchAccess",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
},
{
    "Sid" : "PanoramaAccess",
    "Effect" : "Allow",
    "Action" : [
        "panorama:*"
    ],
    "Resource" : [
        "*"
    ]
}
]

```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon SageMaker gerencie objetos em buckets criados para uso com o Panorama. AWS

### A utilização desta política

Você pode vincular a AWSPanoramaSageMakerRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de dezembro de 2020, 13:13 UTC
- Horário editado: 01 de dezembro de 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "PanoramaSageMakerS3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:GetBucket*"
    ],
    "Resource" : [
      "arn:aws:s3:::*aws-panorama*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaServiceLinkedRolePolicy

AWSPanoramaServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Panorama gerencie recursos em AWS IoT, AWS Secrets Manager e PanoramaAWS.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de outubro de 2021, 12:12 UTC

- Horário editado: 20 de outubro de 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot>DeleteThing",
        "iot>DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot>DeleteCertificate",

```

```
    "iot:AttachPrincipalPolicy",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "PanoramaIoTCreateCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreatePolicy",
    "iot:CreatePolicyVersion",
    "iot:AttachPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:policy/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTJobAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:DescribeJobExecution",
    "iot:CreateJob",
    "iot>DeleteJob"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:job/panorama*",
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
```

```
"Sid" : "PanoramaIoTEndpointAccess",
"Effect" : "Allow",
"Action" : [
  "iot:DescribeEndpoint"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "PanoramaReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "panorama:Describe*",
    "panorama:List*"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "SecretsManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:CreateSecret",
    "secretsmanager:ListSecretVersionIds",
    "secretsmanager>DeleteSecret"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:panorama*",
    "arn:aws:secretsmanager:*:*:secret:Panorama*"
  ]
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy é uma [política AWS gerenciada](#) que: permite que o AWS Panorama gere recursos no Amazon S3, IoT, AWS IoT GreenGrass, LambdaAWS, Amazon SageMaker e Amazon CloudWatch Logs e transmita funções de serviço para IoT, IoT GreenGrass e Amazon SageMaker. AWS IoT

### A utilização desta política

Você pode vincular a AWSPanoramaServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 01 de dezembro de 2020, 13:14 UTC
- Horário editado: 01 de dezembro de 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "iot:CreateThing",
    "iot>DeleteThing",
    "iot>DeleteThingShadow",
    "iot:DescribeThing",
    "iot:GetThingShadow",
    "iot:UpdateThing",
    "iot:UpdateThingShadow"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*"
  ]
},
{
  "Sid" : "PanoramaIoTCertificateAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:AttachThingPrincipal",
    "iot:DetachThingPrincipal",
    "iot:UpdateCertificate",
    "iot>DeleteCertificate",
    "iot:AttachPrincipalPolicy",
    "iot:DetachPrincipalPolicy"
  ],
  "Resource" : [
    "arn:aws:iot:*:*:thing/panorama*",
    "arn:aws:iot:*:*:cert/*"
  ]
},
{
  "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreateKeysAndCertificate",
    "iot:CreatePolicy"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
  "Effect" : "Allow",
  "Action" : [
    "iot:CreatePolicyVersion"
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:iot:*:*:policy/panorama*"
    ]
  },
  {
    "Sid" : "PanoramaIoTJobAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeJobExecution",
      "iot:CreateJob",
      "iot>DeleteJob"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:job/panorama*",
      "arn:aws:iot:*:*:thing/panorama*"
    ]
  },
  {
    "Sid" : "PanoramaIoTEndpointAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:DescribeEndpoint"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "PanoramaAccess",
    "Effect" : "Allow",
    "Action" : [
      "panorama:Describe*",
      "panorama>List*",
      "panorama:Get*"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "PanoramaS3Access",
    "Effect" : "Allow",
    "Action" : [
```

```

    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:DeleteBucket",
    "s3:ListBucket",
    "s3:GetBucket*",
    "s3:CreateBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::*aws-panorama*"
  ]
},
{
  "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "sagemaker.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
    "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
    "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
        "iam:PassedToService" : [
            "greengrass.amazonaws.com"
        ]
    }
}
},
{
    "Sid" : "PanoramaIAMPassIoTRoleAccess",
    "Effect" : "Allow",
    "Action" : [
        "iam:PassRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
    ],
    "Condition" : {
        "StringEqualsIfExists" : {
            "iam:PassedToService" : "iot.amazonaws.com"
        }
    }
},
{
    "Sid" : "PanoramaGreenGrassAccess",
    "Effect" : "Allow",
    "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass>DeleteCoreDefinition",
        "greengrass>DeleteFunctionDefinition",
```

```
"greengrass:DeleteResourceDefinition",
"greengrass:DeleteGroup",
"greengrass:DeleteLoggerDefinition",
"greengrass:DeleteSubscriptionDefinition",
"greengrass:DisassociateRoleFromGroup",
"greengrass:DisassociateServiceRoleFromAccount",
"greengrass:GetAssociatedRole",
"greengrass:GetConnectivityInfo",
"greengrass:GetCoreDefinition",
"greengrass:GetCoreDefinitionVersion",
"greengrass:GetDeploymentStatus",
"greengrass:GetDeviceDefinition",
"greengrass:GetDeviceDefinitionVersion",
"greengrass:GetFunctionDefinition",
"greengrass:GetFunctionDefinitionVersion",
"greengrass:GetGroup",
"greengrass:GetGroupCertificateAuthority",
"greengrass:GetGroupCertificateConfiguration",
"greengrass:GetGroupVersion",
"greengrass:GetLoggerDefinition",
"greengrass:GetLoggerDefinitionVersion",
"greengrass:GetResourceDefinition",
"greengrass:GetServiceRoleForAccount",
"greengrass:GetSubscriptionDefinition",
"greengrass:GetSubscriptionDefinitionVersion",
"greengrass:ListCoreDefinitionVersions",
"greengrass:ListCoreDefinitions",
"greengrass:ListDeployments",
"greengrass:ListDeviceDefinitionVersions",
"greengrass:ListDeviceDefinitions",
"greengrass:ListFunctionDefinitionVersions",
"greengrass:ListFunctionDefinitions",
"greengrass:ListGroupCertificateAuthorities",
"greengrass:ListGroupVersions",
"greengrass:ListGroups",
"greengrass:ListLoggerDefinitionVersions",
"greengrass:ListLoggerDefinitions",
"greengrass:ListSubscriptionDefinitionVersions",
"greengrass:ListSubscriptionDefinitions",
"greengrass:ResetDeployments",
"greengrass:UpdateConnectivityInfo",
"greengrass:UpdateCoreDefinition",
"greengrass:UpdateDeviceDefinition",
"greengrass:UpdateFunctionDefinition",
```

```
    "greengrass:UpdateGroup",
    "greengrass:UpdateGroupCertificateConfiguration",
    "greengrass:UpdateLoggerDefinition",
    "greengrass:UpdateSubscriptionDefinition",
    "greengrass:UpdateResourceDefinition"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "PanoramaLambdaUsersFunctionAccess",
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:*"
  ]
},
{
  "Sid" : "PanoramaSageMakerWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateTrainingJob",
    "sagemaker:StopTrainingJob",
    "sagemaker:CreateCompilationJob",
    "sagemaker:DescribeCompilationJob",
    "sagemaker:StopCompilationJob"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:training-job/panorama*",
    "arn:aws:sagemaker:*:*:compilation-job/panorama*"
  ]
},
{
  "Sid" : "PanoramaSageMakerListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListCompilationJobs"
  ]
},
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "PanoramaSageMakerReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:DescribeTrainingJob"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:training-job/*"
    ]
  },
  {
    "Sid" : "PanoramaCWLogsAccess",
    "Effect" : "Allow",
    "Action" : [
      "iot:AttachPolicy",
      "iot:CreateRoleAlias"
    ],
    "Resource" : [
      "arn:aws:iot:*:*:policy/panorama*",
      "arn:aws:iot:*:*:rolealias/panorama*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSPriceListServiceFullAccess

AWSPriceListServiceFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Serviço de Lista de AWS Preços.

## A utilização desta política

Você pode vincular a AWSPriceListServiceFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de novembro de 2017, 00:36 UTC
- Horário editado: 22 de novembro de 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPRivateCAAuditor

AWSPRivateCAAuditor é uma [política AWS gerenciada](#) que: Fornece acesso do auditor à Autoridade de Certificação AWS Privada

### A utilização desta política

Você pode vincular a AWSPRivateCAAuditor aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de fevereiro de 2023, 18:33 UTC
- Horário editado: 14 de fevereiro de 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAAuditor`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:CreateCertificateAuthorityAuditReport",
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:ListCertificateAuthorities"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPriateCAFullAccess

AWSPriateCAFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à Autoridade de Certificação AWS Privada

## A utilização desta política

Você pode vincular a `AWSPriateCAFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de fevereiro de 2023, 18:20 UTC
- Horário editado: 14 de fevereiro de 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriateCAFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPRivateCAPrivilegedUser

AWSPRivateCAPrivilegedUser é uma [política AWS gerenciada](#) que: Fornece acesso privilegiado de usuários certificados à Autoridade de Certificação AWS Privada

### A utilização desta política

Você pode vincular a AWSPRivateCAPrivilegedUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de fevereiro de 2023, 18:26 UTC
- Horário editado: 14 de fevereiro de 2023, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAPrivilegedUser`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPprivateCAReadOnly

AWSPprivateCAReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura à Autoridade de Certificação AWS Privada

### A utilização desta política

Você pode vincular a AWSPprivateCAReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de fevereiro de 2023, 18:30 UTC
- Horário editado: 14 de fevereiro de 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPprivateCAReadOnly`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"acm-pca:DescribeCertificateAuthority",
"acm-pca:DescribeCertificateAuthorityAuditReport",
"acm-pca:ListCertificateAuthorities",
"acm-pca:GetCertificateAuthorityCsr",
"acm-pca:GetCertificateAuthorityCertificate",
"acm-pca:GetCertificate",
"acm-pca:GetPolicy",
"acm-pca:ListPermissions",
"acm-pca:ListTags"
],
"Resource" : "*"
}
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPRivateCAUser

AWSPRivateCAUser é uma [política AWS gerenciada](#) que: Fornece ao usuário certificado acesso à Autoridade de Certificação AWS Privada

## A utilização desta política

Você pode vincular a AWSPRivateCAUser aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de fevereiro de 2023, 18:16 UTC
- Horário editado: 14 de fevereiro de 2023, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPRivateCAUser`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total a todas as ações administrativas de um AWS Private Marketplace.

### Utilização desta política

Você pode vincular a AWSPrivateMarketplaceAdminFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 27 de novembro de 2018, 16:32 UTC
- Horário editado: 14 de fevereiro de 2024, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AWSPriveteMarketplaceRequests

AWSPriveteMarketplaceRequests é uma [política AWS gerenciada](#) que: Fornece acesso à criação de solicitações em um Marketplace AWS privado.

## A utilização desta política

Você pode vincular a AWSPriveteMarketplaceRequests aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 28 de outubro de 2019, 21:44 UTC
- Horário editado: 28 de outubro de 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriveteMarketplaceRequests`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPrivateNetworksServiceRolePolicy

AWSPrivateNetworksServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Private Networks Service gerencie recursos em nome do cliente.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de dezembro de 2021, 23:17 UTC
- Horário editado: 16 de dezembro de 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonCodeBuildProvisioningBasicAccess

AWSProtonCodeBuildProvisioningBasicAccess é uma [política AWS gerenciada](#) que: Permissões que o CodeBuild precisa para executar uma compilação para o Proton CodeBuild ProvisioningAWS.

### A utilização desta política

Você pode vincular a AWSProtonCodeBuildProvisioningBasicAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 09 de novembro de 2022, 21:04 UTC
- Horário editado: 09 de novembro de 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)



- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonCodeBuildProvisioningServiceRolePolicy

AWSProtonCodeBuildProvisioningServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS Proton gerencie o provisionamento de recursos do Proton usando o CodeBuild e outros serviços em seu nome. AWS

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de novembro de 2022, 21:32 UTC
- Horário editado: 17 de maio de 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Action" : [
  "cloudformation:CreateStack",
  "cloudformation:CreateChangeSet",
  "cloudformation>DeleteChangeSet",
  "cloudformation>DeleteStack",
  "cloudformation:UpdateStack",
  "cloudformation:DescribeStacks",
  "cloudformation:DescribeStackEvents",
  "cloudformation:ListStackResources"
],
"Resource" : [
  "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "codebuild:CreateProject",
    "codebuild>DeleteProject",
    "codebuild:UpdateProject",
    "codebuild:StartBuild",
    "codebuild:StopBuild",
    "codebuild:RetryBuild",
    "codebuild:BatchGetBuilds",
    "codebuild:BatchGetProjects"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "codebuild.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicequotas:GetServiceQuota"
  ],
  "Resource" : "*"
}
```

```
}  
]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonDeveloperAccess

AWSProtonDeveloperAccess é uma [política AWS gerenciada](#) que: fornece acesso às APIs e ao console de gerenciamento do AWS Proton, mas não permite a administração de modelos ou ambientes do Proton.

### A utilização desta política

Você pode vincular a AWSProtonDeveloperAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de fevereiro de 2021, 19:02 UTC
- Horário editado: 18 de novembro de 2022, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "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" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
  "Condition" : {
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSProtonFullAccess

AWSProtonFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total às APIs do AWS Proton e ao console de gerenciamento. Além dessas permissões, o acesso ao Amazon S3 também é necessário para registrar pacotes de modelos de seus buckets do S3, bem como o acesso ao Amazon IAM para criar e gerenciar as funções de serviço do Proton.

## A utilização desta política

Você pode vincular a AWSProtonFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de fevereiro de 2021, 19:07 UTC
- Horário editado: 20 de junho de 2022, 12:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ]
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "proton.*.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "proton.amazonaws.com"
      }
    }
  },
  {
    "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"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:PassConnection"
    ],
    "Resource" : "arn:aws:codestar-connections::*:connection/*",
    "Condition" : {
```

```
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonReadOnlyAccess

AWSProtonReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura às APIs do AWS Proton e ao console de gerenciamento.

### A utilização desta política

Você pode vincular a AWSProtonReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de fevereiro de 2021, 19:09 UTC
- Horário editado: 18 de novembro de 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",

```

```
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListRepositories",
    "proton:ListRepositorySyncDefinitions",
    "proton:ListServiceInstanceOutputs",
    "proton:ListServiceInstanceProvisionedResources",
    "proton:ListServiceInstances",
    "proton:ListServicePipelineOutputs",
    "proton:ListServicePipelineProvisionedResources",
    "proton:ListServices",
    "proton:ListServiceTemplateMajorVersions",
    "proton:ListServiceTemplateMinorVersions",
    "proton:ListServiceTemplates",
    "proton:ListServiceTemplateVersions",
    "proton:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonServiceGitSyncServiceRolePolicy

AWSProtonServiceGitSyncServiceRolePolicy é uma [política AWS gerenciada](#) que: Política que permite ao AWS Proton sincronizar suas definições de serviço, ambiente e componente do seu repositório git com o Proton. AWS

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de abril de 2023, 15:55 UTC
- Horário editado: 04 de abril de 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ]
    }
  ]
}
```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy é uma [política gerenciada da AWS](#) que: Política que permite ao AWS Proton sincronizar o conteúdo do repositório git com o Proton ou sincronizar o conteúdo do Proton com seus repositórios git.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de novembro de 2021, 21:14 UTC
- Horário editado: 23 de novembro de 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton>DeleteServiceTemplateVersion",
        "proton>DeleteEnvironmentTemplateVersion",
        "proton>CreateServiceTemplateVersion",
        "proton>CreateServiceTemplate",
        "proton>CreateEnvironmentTemplateVersion",
        "proton>CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton>CreateEnvironmentTemplateMajorVersion",
        "proton>CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy é uma [política AWS gerenciada](#) que: Concede permissões para visualizar e modificar pedidos de compra no console de cobrança

### A utilização desta política

Você pode vincular a AWSPurchaseOrdersServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de maio de 2020, 18:15 UTC
- Horário editado: 17 de julho de 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSQuicksightAthenaAccess

AWSQuicksightAthenaAccess é uma [política AWS gerenciada](#) que: acesso rápido à API do Athena e aos buckets do S3 usados para resultados de consultas do Athena

## A utilização desta política

Você pode vincular a AWSQuicksightAthenaAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de dezembro de 2016, 02:31 UTC
- Horário editado: 07 de julho de 2021, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

## Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
```



```
    "athena:GetQueryExecutions",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetTable",
    "athena:GetTables",
    "athena:ListQueryExecutions",
    "athena:RunQuery",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution",
    "athena:ListWorkGroups",
    "athena:ListEngineVersions",
    "athena:GetWorkGroup",
    "athena:GetDataCatalog",
    "athena:GetDatabase",
    "athena:GetTableMetadata",
    "athena:ListDataCatalogs",
    "athena:ListDatabases",
    "athena:ListTableMetadata"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue: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" : [
    "*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSQuickSightDescribeRDS

AWSQuickSightDescribeRDS é uma [política AWS gerenciada](#) que: Permitir que o QuickSight descreva os recursos do RDS

## A utilização desta política

Você pode vincular a AWSQuickSightDescribeRDS aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 10 de novembro de 2015, 23:24 UTC
- Horário editado: 10 de novembro de 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSQuickSightDescribeRedshift

AWSQuickSightDescribeRedshift é uma [política AWS gerenciada](#) que: Permitir que o QuickSight descreva os recursos do Redshift

### A utilização desta política

Você pode vincular a AWSQuickSightDescribeRedshift aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 10 de novembro de 2015, 23:25 UTC
- Horário editado: 10 de novembro de 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos recursos do Amazon Elasticsearch do Amazon QuickSight

### A utilização desta política

Você pode vincular a AWSQuickSightElasticsearchPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 09 de setembro de 2020, 17:27 UTC
- Horário editado: 07 de setembro de 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
```

```
    "es:ESHttpGet"
  ],
  "Resource" : [
    "arn:aws:es:*:*:domain/*/_opendistro/_sql",
    "arn:aws:es:*:*:domain/*/_plugin/_sql"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSQuickSightIoTAnalyticsAccess

AWSQuickSightIoTAnalyticsAccess é uma [política AWS gerenciada](#) que: Dê ao QuickSight acesso somente de leitura aos conjuntos de dados do IoT Analytics

### A utilização desta política

Você pode vincular a AWSQuickSightIoTAnalyticsAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 17:00 UTC
- Horário editado: 29 de novembro de 2017, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSQuickSightListIAM

AWSQuickSightListIAM é uma [política AWS gerenciada](#) que: Permitir que o QuickSight liste entidades do IAM

## A utilização desta política

Você pode vincular a AWSQuickSightListIAM aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 10 de novembro de 2015, 23:25 UTC
- Horário editado: 10 de novembro de 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSQuicksightOpenSearchPolicy

AWSQuicksightOpenSearchPolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos recursos do Amazon OpenSearch do Amazon QuickSight

## A utilização desta política

Você pode vincular a AWSQuicksightOpenSearchPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 07 de setembro de 2021, 23:26 UTC
- Horário editado: 07 de setembro de 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : "es:ListDomainNames",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "es:DescribeDomain"
  ],
  "Resource" : [
    "arn:aws:es:*:*:domain/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "es:ESHttpPost",
    "es:ESHttpGet"
  ],
  "Resource" : [
    "arn:aws:es:*:*:domain/*/_opendistro/_sql",
    "arn:aws:es:*:*:domain/*/_plugin/_sql"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSQuickSightSageMakerPolicy

AWSQuickSightSageMakerPolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos recursos do Amazon SageMaker a partir do Amazon QuickSight

## A utilização desta política

Você pode vincular a `AWSQuickSightSageMakerPolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 17 de janeiro de 2020, 17:18 UTC
- Horário editado: 30 de outubro de 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModel",

```

```
    "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*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSQuickSightTimestreamPolicy

AWSQuickSightTimestreamPolicy é uma [política AWS gerenciada](#) que: acesso AWS QuickSight às APIs do AWS Timestream. Os clientes podem anexar essa política à função AWS QuickSight para permitir a recuperação de dados e metadados.

## A utilização desta política

Você pode vincular a AWSQuickSightTimestreamPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 30 de setembro de 2020, 21:47 UTC
- Horário editado: 30 de setembro de 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
```

```
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSReachabilityAnalyzerServiceRolePolicy

AWSReachabilityAnalyzerServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o VPC Reachability Analyzer AWS acesse recursos e se integre às Organizations em seu nome. AWS

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de novembro de 2022, 17:12 UTC
- Horário editado: 23 de junho de 2023, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRefactoringToolkitFullAccess

`AWSRefactoringToolkitFullAccess` é uma [política gerenciada pela AWS](#): Essa política concede permissão para usar serviços AWS com a extensão AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. Ele deve ser anexado a um AWS perfil local. A política permite o upload de artefatos do aplicativo e o download dos artefatos resultantes do Amazon S3. Ele permite criar aplicativos em uma imagem de contêiner usando, armazenar AWS CodeBuild e recuperar as imagens do Amazon Elastic Container Registry (Amazon ECR). Além disso, permite a implantação do aplicativo em serviços de contêineres na AWS, como o Amazon Elastic Container Service (Amazon ECS), a criação opcional de recursos de VPC, a conexão opcional à infraestrutura existente, como o Directory AWS Service, e outros serviços relacionados.

## Utilização desta política

Você pode vincular a `AWSRefactoringToolkitFullAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 25 de outubro de 2022, 16:41 UTC
- Horário editado: 18 de novembro de 2023, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRefactoringToolkitSidecarPolicy

AWSRefactoringToolkitSidecarPolicy é uma [política AWS gerenciada](#) que: Essa política deve ser usada pelas tarefas do Amazon ECS criadas para testar aplicativos AWS usando a extensão AWS Toolkit for .NET Refactoring para Microsoft Visual Studio. A política concede acesso para baixar artefatos do aplicativo do Amazon S3, comunicar o status da tarefa usando o Systems Manager e outros serviços necessários.

### A utilização desta política

Você pode vincular a AWSRefactoringToolkitSidecarPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 25 de outubro de 2022, 16:41 UTC
- Horário editado: 29 de outubro de 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Sid" : "SsmMessagesAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssmmessages:OpenControlChannel",
    "ssmmessages:CreateControlChannel",
    "ssmmessages:OpenDataChannel",
    "ssmmessages:CreateDataChannel"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3GetObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3::*/refactoringtoolkit*"
},
{
  "Sid" : "S3ListBucketAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : "refactoringtoolkit*"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSrePostPrivateCloudWatchAccess

AWSrePostPrivateCloudWatchAccess é uma [política AWS gerenciada](#) que: Fornece acesso privado ao re:POST para publicar dados de métricas CloudWatch

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de novembro de 2023, 16:37 UTC
- Hora da edição: 15 de novembro de 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

```
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/rePostPrivate",
          "AWS/Usage"
        ]
      }
    }
  }
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicy é uma [política AWS gerenciada](#) que: Essa política permite que o serviço re:Post Space crie, gerencie e resolva casos de Support criados por meio do aplicativo Space.

### Utilização desta política

Você pode vincular a AWSRepostSpaceSupportOperationsPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 26 de novembro de 2023, 21:52 UTC
- Horário editado: 26 de novembro de 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSResilienceHubAssessmentExecutionPolicy

AWSResilienceHubAssessmentExecutionPolicy é uma [política AWS gerenciada](#) que: Policy for AWS Resilience Hub, função de serviço que permite acesso a outros AWS serviços para executar a avaliação.

## A utilização desta política

Você pode vincular a AWSResilienceHubAssessmentExecutionPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2023, 12:32 UTC
- Horário editado: 29 de outubro de 2023, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
```

```
"backup:GetBackupSelection",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"cloudformation:DescribeStacks",
"cloudformation:ListStackResources",
"cloudformation:ValidateTemplate",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics",
"devops-guru:ListMonitoredResources",
"dlm:GetLifecyclePolicies",
"dlm:GetLifecyclePolicy",
"drs:DescribeJobs",
"drs:DescribeSourceServers",
"drs:GetReplicationConfiguration",
"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",
"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",
"s3:GetBucketLocation",
"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/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Resource Access Manager

## A utilização desta política

Você pode vincular a `AWSResourceAccessManagerFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de junho de 2019, 17:28 UTC
- Horário editado: 04 de junho de 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS Resource Access Manager.

### A utilização desta política

Você pode vincular a AWSResourceAccessManagerReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de dezembro de 2019, 20:58 UTC
- Horário editado: 09 de dezembro de 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess é uma [política AWS gerenciada](#) que: Fornece acesso às APIs do AWS Resource Access Manager necessárias para um participante do compartilhamento de recursos.

### A utilização desta política

Você pode vincular a AWSResourceAccessManagerResourceShareParticipantAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de dezembro de 2019, 20:41 UTC
- Horário editado: 09 de dezembro de 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceAccessManagerServiceRolePolicy

`AWSResourceAccessManagerServiceRolePolicy` é uma [política AWS gerenciada que: Política](#) contendo acesso somente de leitura do AWS Resource Access Manager à estrutura de organizações dos clientes. Ela também contém permissões do IAM para excluir a função.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de novembro de 2018, 19:28 UTC
- Horário editado: 14 de novembro de 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess é uma [política gerenciada pela AWS](#): Essa política concede permissões administrativas para acessar os recursos do Resource Explorer e concede permissões somente de leitura a outros serviços da AWS para oferecer suporte a esse acesso.

### Utilização desta política

Você pode vincular a AWSResourceExplorerFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 07 de novembro de 2022, 20:01 UTC
- Hora da edição: 14 de novembro de 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceExplorerOrganizationsAccess

AWSResourceExplorerOrganizationsAccess é uma [política gerenciada pela AWS](#): Essa política concede permissões administrativas ao Resource Explorer e concede permissões somente de leitura a outros serviços da AWS para oferecer suporte a esse acesso. O administrador do AWS Organizations precisa dessas permissões para configurar e gerenciar a pesquisa em várias contas no console.

### Utilização desta política

Você pode vincular a AWSResourceExplorerOrganizationsAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 14 de novembro de 2023, 17:01 UTC
- Hora da edição: 14 de novembro de 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Sid" : "OrganizationsAdministratorAccess",
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "resource-explorer-2.amazonaws.com"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceExplorerReadOnlyAccess

`AWSResourceExplorerReadOnlyAccess` é uma [política gerenciada pela AWS](#): Essa política concede permissões somente de leitura para pesquisar e visualizar recursos do Resource Explorer e concede permissões somente de leitura a outros serviços da AWS para oferecer suporte a esse acesso.

## Utilização desta política

Você pode vincular a `AWSResourceExplorerReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 07 de novembro de 2022, 19:56 UTC
- Hora da edição: 14 de novembro de 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Resource Explorer visualize recursos e CloudTrail eventos em seu nome para indexar seus recursos para pesquisa.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 25 de outubro de 2022, 20:35 UTC
- Horário editado: 20 de dezembro de 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "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:GetEntityTypes",
"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",
"resiliencehub:ListApps",
"resiliencehub: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" : [
```

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSResourceGroupsReadOnlyAccess

`AWSResourceGroupsReadOnlyAccess` é uma [política AWS gerenciada](#) que: Esta é a política somente de leitura para AWS Resource Groups

### A utilização desta política

Você pode vincular a `AWSResourceGroupsReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de março de 2018, 10:27 UTC
- Horário editado: 05 de fevereiro de 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
```

```
    "storagegateway:ListGateways",
    "storagegateway:DescribeGatewayInformation",
    "storagegateway:ListTagsForResource",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "ssm:ListDocuments"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRoboMaker\_FullAccess

AWSRoboMaker\_FullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS RoboMaker por meio do AWS Management Console e SDK. Também fornece acesso selecionado a serviços relacionados (por exemplo, S3, IAM).

### A utilização desta política

Você pode vincular a AWSRoboMaker\_FullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 10 de setembro de 2020, 18:34 UTC
- Horário editado: 16 de setembro de 2021, 21:06 UTC

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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "ecr-public:DescribeImages",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:CalledViaFirst" : "robomaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "robomaker.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRoboMakerReadOnlyAccess

`AWSRoboMakerReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao AWS RoboMaker por meio do AWS Management Console e SDK

## A utilização desta política

Você pode vincular a `AWSRoboMakerReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de novembro de 2018, 05:30 UTC
- Horário editado: 28 de agosto de 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRoboMakerServicePolicy

AWSRoboMakerServicePolicy é uma [política AWS gerenciada que: política](#) de serviço do RoboMaker

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2018, 06:30 UTC
- Horário editado: 11 de novembro de 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
```

```

    "ec2:DescribeVpcs",
    "ec2:DescribeSecurityGroups",
    "greengrass:CreateDeployment",
    "greengrass:CreateGroupVersion",
    "greengrass:CreateFunctionDefinition",
    "greengrass:CreateFunctionDefinitionVersion",
    "greengrass:GetDeploymentStatus",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetFunctionDefinitionVersion",
    "greengrass:GetAssociatedRole",
    "lambda:CreateFunction",
    "robomaker:CreateSimulationJob",
    "robomaker:CancelSimulationJob"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Action" : [
    "robomaker:TagResource"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
},
{
  "Action" : [
    "lambda:UpdateFunctionCode",
    "lambda:GetFunction",
    "lambda:UpdateFunctionConfiguration",
    "lambda>DeleteFunction",
    "lambda:ListVersionsByFunction",
    "lambda:GetAlias",
    "lambda:UpdateAlias",
    "lambda:CreateAlias",
    "lambda>DeleteAlias"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",

```

```
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "lambda.amazonaws.com",
      "robomaker.amazonaws.com"
    ]
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRoboMakerServiceRolePolicy

AWSRoboMakerServiceRolePolicy é uma [política AWS gerenciada que: política](#) de serviço do RoboMaker

### A utilização desta política

Você pode vincular a AWSRoboMakerServiceRolePolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de novembro de 2018, 05:33 UTC
- Horário editado: 26 de novembro de 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "lambda.amazonaws.com"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSRolesAnywhereServicePolicy

AWSRolesAnywhereServicePolicy é uma [política AWS gerenciada](#) que: permite que o IAM Roles Anywhere publique métricas de serviço/uso no CloudWatch e verifique o status das autoridades de certificação privadas em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de julho de 2022, 15:26 UTC
- Horário editado: 05 de julho de 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o serviço Amazon S3 on Outposts gerencie recursos de rede EC2 em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 03 de outubro de 2023, 20:32 UTC
- Horário editado: 03 de outubro de 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "ec2:DescribeSecurityGroups",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeVpcs",
    "ec2:DescribeCoipPools",
    "ec2:GetCoipPoolUsage",
    "ec2:DescribeAddresses",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
  ],
  "Resource" : "*",
  "Sid" : "DescribeVpcResources"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Sid" : "CreateNetworkInterface"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "S3 On Outposts"
    }
  },
  "Sid" : "CreateTagsForCreateNetworkInterface"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:ipv4pool-ec2/*"
  ]
}

```

```
    ],
    "Sid" : "AllocateIpAddress"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "S3 On Outposts"
      }
    },
    "Sid" : "CreateTagsForAllocateIpAddress"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress",
      "ec2:AssociateAddress"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
      }
    },
    "Sid" : "ReleaseVpcResources"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "*",
    "Condition" : {
```

```
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateNetworkInterface",
        "AllocateAddress"
      ],
      "aws:RequestTag/CreatedBy" : [
        "S3 On Outposts"
      ]
    }
  },
  "Sid" : "CreateTags"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSavingsPlansFullAccess

AWSSavingsPlansFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço Savings Plans

### A utilização desta política

Você pode vincular a AWSSavingsPlansFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de novembro de 2019, 22:45 UTC
- Horário editado: 06 de novembro de 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao serviço Savings Plans

## A utilização desta política

Você pode vincular a AWSSavingsPlansReadOnlyAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de novembro de 2019, 22:45 UTC
- Horário editado: 06 de novembro de 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSecurityHubFullAccess

AWSecurityHubFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total para usar o AWS Security Hub.

## Utilização desta política

Você pode vincular a AWSecurityHubFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 27 de novembro de 2018, 23:54 UTC
- Horário editado: 16 de novembro de 2023, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSecurityHubOrganizationsAccess

AWSecurityHubOrganizationsAccess é uma [política gerenciada pela AWS](#) que: concede permissão para habilitar e gerenciar o AWS Security Hub em uma organização. Inclui habilitar o serviço em toda a organização e determinar a conta de administrador delegado para o serviço.

## Utilização desta política

Você pode vincular a AWSecurityHubOrganizationsAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 15 de março de 2021, 20:53 UTC
- Horário editado: 16 de novembro de 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations: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"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSecurityHubReadOnlyAccess

AWSSecurityHubReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do AWS Security Hub

## Utilização desta política

Você pode vincular a `AWSecurityHubReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 28 de novembro de 2018, 01:34 UTC
- Horário editado: 22 de fevereiro de 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy é uma [política gerenciada pela AWS](#): É necessária uma função vinculada ao serviço para que o AWS Security Hub acesse seus recursos.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de novembro de 2018, 23:47 UTC
- Horário editado: 27 de novembro de 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

### Versão da política

Versão da política: v14 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "SecurityHubServiceRolePermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:DescribeTrails",
      "cloudtrail:GetTrailStatus",
      "cloudtrail:GetEventSelectors",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:DescribeAlarmsForMetric",
      "logs:DescribeMetricFilters",
      "sns:ListSubscriptionsByTopic",
      "config:DescribeConfigurationRecorders",
      "config:DescribeConfigurationRecorderStatus",
      "config:DescribeConfigRules",
      "config:DescribeConfigRuleEvaluationStatus",
      "config:BatchGetResourceConfig",
      "config>SelectResourceConfig",
      "iam:GenerateCredentialReport",
      "organizations:ListAccounts",
      "config:PutEvaluations",
      "tag:GetResources",
      "iam:GetCredentialReport",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListChildren",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeOrganizationalUnit",
      "securityhub:BatchDisableStandards",
      "securityhub:BatchEnableStandards",
      "securityhub:BatchUpdateStandardsControlAssociations",
      "securityhub:BatchGetSecurityControls",
      "securityhub:BatchGetStandardsControlAssociations",
      "securityhub>CreateMembers",
      "securityhub>DeleteMembers",
      "securityhub:DescribeHub",
      "securityhub:DescribeOrganizationConfiguration",
      "securityhub:DescribeStandards",
      "securityhub:DescribeStandardsControls",
      "securityhub:DisassociateFromAdministratorAccount",
      "securityhub:DisassociateMembers",
      "securityhub:DisableSecurityHub",
      "securityhub:EnableSecurityHub",
```



```

    "securityhub:GetEnabledStandards",
    "securityhub:ListStandardsControlAssociations",
    "securityhub:ListSecurityControlDefinitions",
    "securityhub:UpdateOrganizationConfiguration",
    "securityhub:UpdateSecurityControl",
    "securityhub:UpdateSecurityHubConfiguration",
    "securityhub:UpdateStandardsControl"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SecurityHubServiceRoleConfigPermissions",
  "Effect" : "Allow",
  "Action" : [
    "config:PutConfigRule",
    "config>DeleteConfigRule",
    "config:GetComplianceDetailsByConfigRule"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
},
{
  "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "securityhub.amazonaws.com"
      ]
    }
  }
}
]
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogAdminFullAccess

AWSServiceCatalogAdminFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total aos recursos administrativos do catálogo de serviços

### A utilização desta política

Você pode vincular a AWSServiceCatalogAdminFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de fevereiro de 2018, 17:19 UTC
- Horário editado: 13 de abril de 2023, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
```

```

    "cloudformation:SetStackPolicy",
    "cloudformation:UpdateStack",
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation>DeleteChangeSet",
    "cloudformation:ListStackResources",
    "cloudformation:TagResource",
    "cloudformation>CreateStackSet",
    "cloudformation>CreateStackInstances",
    "cloudformation:UpdateStackSet",
    "cloudformation:UpdateStackInstances",
    "cloudformation>DeleteStackSet",
    "cloudformation>DeleteStackInstances",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateUploadBucket",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ValidateTemplate",
    "iam:GetGroup",
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListGroups",
    "iam:ListRoles",
    "iam:ListUsers",
    "servicecatalog:Get*",
    "servicecatalog:Scan*",
    "servicecatalog:Search*"
  ]
}

```

```
    "servicecatalog:List*",
    "servicecatalog:TagResource",
    "servicecatalog:UntagResource",
    "servicecatalog:SyncResource",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:ListDocumentVersions",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:Accept*",
    "servicecatalog:Associate*",
    "servicecatalog:Batch*",
    "servicecatalog:Copy*",
    "servicecatalog:Create*",
    "servicecatalog>Delete*",
    "servicecatalog:Describe*",
    "servicecatalog:Disable*",
    "servicecatalog:Disassociate*",
    "servicecatalog:Enable*",
    "servicecatalog:Execute*",
    "servicecatalog:Import*",
    "servicecatalog:Provision*",
    "servicecatalog:Put*",
    "servicecatalog:Reject*",
    "servicecatalog:Terminate*",
    "servicecatalog:Update*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "servicecatalog.amazonaws.com"
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogAdminReadOnlyAccess

AWSServiceCatalogAdminReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura aos recursos administrativos do Service Catalog

### A utilização desta política

Você pode vincular a AWSServiceCatalogAdminReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de outubro de 2019, 18:53 UTC
- Horário editado: 25 de outubro de 2019, 18:53 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:::stack/SC-*",
        "arn:aws:cloudformation:::stack/StackSet-SC-*",
        "arn:aws:cloudformation:::changeSet/SC-*",
        "arn:aws:cloudformation:::stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",

```

```
    "iam:GetRole",
    "iam:GetUser",
    "iam:ListGroups",
    "iam:ListRoles",
    "iam:ListUsers",
    "servicecatalog:Get*",
    "servicecatalog:List*",
    "servicecatalog:Describe*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:Search*",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:ListDocuments",
    "ssm:ListDocumentVersions",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccess é uma [política gerenciada pela AWS](#): fornece acesso total aos recursos do Service Catalog App Registry

### Utilização desta política

Você pode vincular a AWSServiceCatalogAppRegistryFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 12 de novembro de 2020, 22:25 UTC
- Horário editado: 07 de dezembro de 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups>DeleteGroup",
```



```

    "resource-groups:GetGroup",
    "resource-groups:GetTags",
    "resource-groups:Tag",
    "resource-groups:Untag",
    "resource-groups:GetGroupConfiguration",
    "resource-groups:AssociateResource",
    "resource-groups:DisassociateResource"
  ],
  "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
    }
  }
},
{
  "Sid" : "AppRegistryServiceLinkedRole",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam:*:*:role/aws-service-role/servicecatalog-appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
    }
  }
},
{
  "Sid" : "AppRegistryOperations",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "servicecatalog:CreateApplication",
    "servicecatalog:GetApplication",
    "servicecatalog:UpdateApplication",
    "servicecatalog>DeleteApplication",
    "servicecatalog>ListApplications",
    "servicecatalog:AssociateResource",
    "servicecatalog:DisassociateResource",
    "servicecatalog:GetAssociatedResource",
    "servicecatalog>ListAssociatedResources",
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup",
    "servicecatalog>ListAssociatedAttributeGroups",
  ]
}

```

```
    "servicecatalog:CreateAttributeGroup",
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog>DeleteAttributeGroup",
    "servicecatalog:GetAttributeGroup",
    "servicecatalog>ListAttributeGroups",
    "servicecatalog:SyncResource",
    "servicecatalog>ListAttributeGroupsForApplication",
    "servicecatalog:GetConfiguration",
    "servicecatalog:PutConfiguration"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AppRegistryResourceTagging",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:ListTagsForResource",
    "servicecatalog:UntagResource",
    "servicecatalog:TagResource"
  ],
  "Resource" : "arn:aws:servicecatalog:*:*:*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogAppRegistryReadOnlyAccess

AWSServiceCatalogAppRegistryReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura aos recursos do Service Catalog App Registry

## A utilização desta política

Você pode vincular a `AWSServiceCatalogAppRegistryReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 12 de novembro de 2020, 22:34 UTC
- Horário editado: 17 de novembro de 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogAppRegistryServiceRolePolicy

AWSServiceCatalogAppRegistryServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Service Catalog AppRegistry gerencie Resource Groups em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora de criação: 18 de maio de 2021, 22:18 UTC
- Horário editado: 26 de outubro de 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups>DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
```

```
    "resource-groups:GetGroupConfiguration"
  ],
  "Resource" : [
    "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
    "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
  ]
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total aos recursos do usuário final do catálogo de serviços

### A utilização desta política

Você pode vincular a AWSServiceCatalogEndUserFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de fevereiro de 2018, 17:22 UTC
- Horário editado: 10 de julho de 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation>DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",

```

```

    "arn:aws:cloudformation:*:*:stackset/SC-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog>CreateProvisionedProductPlan",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ExecuteProvisionedProductPlan",
    "servicecatalog>DeleteProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteProvisionedProductServiceAction",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}

```



```
    }  
  }  
} ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogEndUserReadOnlyAccess

AWSServiceCatalogEndUserReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos recursos do usuário final do Service Catalog

### A utilização desta política

Você pode vincular a AWSServiceCatalogEndUserReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de outubro de 2019, 18:49 UTC
- Horário editado: 25 de outubro de 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",

```

```
    "config:DescribeConfigurationRecorderStatus"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:DescribeServiceActionExecutionParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSServiceCatalogOrgsDataSyncServiceRolePolicy

AWSServiceCatalogOrgsDataSyncServiceRolePolicy é uma [política AWS gerenciada que: Uma política](#) de funções vinculadas ao serviço para que o AWS ServiceCatalog sincronize com a estrutura organizacional da Organizations AWS

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 10 de abril de 2023, 20:48 UTC
- Horário editado: 10 de abril de 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
```

```
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceCatalogSyncServiceRolePolicy

AWSServiceCatalogSyncServiceRolePolicy é uma [política AWS gerenciada](#) que: Uma função vinculada ao serviço para que o AWS ServiceCatalog sincronize artefatos de provisionamento dos repositórios de origem

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de novembro de 2022, 21:20 UTC
- Horário editado: 15 de novembro de 2022, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog>DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog>CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForAmazonEKSNodegroup

`AWSServiceRoleForAmazonEKSNodegroup` é uma [política gerenciada pela AWS](#) que: Permissões necessárias para gerenciar grupos de nós na conta do cliente. Essas políticas estão relacionadas ao gerenciamento dos seguintes recursos: `AutoscalingGroups` `SecurityGroups`, `LaunchTemplates` `InstanceProfiles` e.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de novembro de 2019, 01:34 UTC
- Horário editado: 04 de janeiro de 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
```



```

    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/eks:nodegroup-name" : "*"
      }
    }
  },
  {
    "Sid" : "AutoscalingRelatedPermissions",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:DeleteAutoScalingGroup",
      "autoscaling:TerminateInstanceInAutoScalingGroup",
      "autoscaling:CompleteLifecycleAction",
      "autoscaling:PutLifecycleHook",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:EnableMetricsCollection"
    ],
    "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/*"
      ]
    }
  }
}
]
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos recursos do Systems Manager usados pelo CloudWatch Alarms

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 01 de outubro de 2020, 09:49 UTC
- Horário editado: 01 de outubro de 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICERolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForCloudWatchMetrics\_DbPerfInsightsServiceRolePolicy

AWSServiceRoleForCloudWatchMetrics\_DbPerfInsightsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o CloudWatch acesse as métricas do RDS Performance Insights em seu nome

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de setembro de 2023, 09:32 UTC
- Horário editado: 07 de setembro de 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForCodeGuru-Profiler

AWSServiceRoleForCodeGuru-Profiler é uma [política AWS gerenciada](#) que: É necessária uma função vinculada ao serviço para que o Amazon CodeGuru Profiler envie notificações em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de junho de 2020, 22:04 UTC
- Horário editado: 26 de junho de 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuruProfiler`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForCodeWhispererPolicy

AWSServiceRoleForCodeWhispererPolicy é uma [política AWS gerenciada](#) que: Essa função concede permissões CodeWhisperer para acessar dados em sua conta para calcular o faturamento, fornece acesso para criar e acessar relatórios de segurança na Amazon CodeGuru e emitir dados para. CloudWatch

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de março de 2023, 19:39 UTC
- Horário editado: 01 de março de 2024, 23:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance"
      ],
      "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"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSServiceRoleForEC2ScheduledInstances

AWSServiceRoleForEC2ScheduledInstances é uma [política AWS gerenciada](#) que: permite que instâncias programadas do EC2 iniciem e gerenciem instâncias spot.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de outubro de 2017, 18:31 UTC
- Horário editado: 12 de outubro de 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy é uma [política AWS gerenciada](#) que: A AWS GroundStation usa essa função vinculada ao serviço para invocar o EC2 para encontrar endereços IPv4 públicos

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 13 de dezembro de 2022, 23:52 UTC

- Horário editado: 13 de dezembro de 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForImageBuilder

AWSServiceRoleForImageBuilder é uma [política AWS gerenciada](#) que: Permite que o EC2ImageBuilder chame AWS serviços em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2019, 22:02 UTC
- Horário editado: 19 de outubro de 2023, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

### Versão da política

Versão da política: v19 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "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:DescribeInstanceState",
        "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-*"
    ]
  }
}
```

```
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForIoTSiteWise

`AWSServiceRoleForIoTSiteWise` é uma [política AWS gerenciada](#) que: permite que SiteWise a AWS IoT provisione e gerencie gateways, bem como consulte dados. A política inclui as permissões necessárias do AWS Greengrass para implantação em grupos, permissões do AWS Lambda para criar e atualizar funções com prefixo de serviço e permissões do AWS IoT Analytics para consultar dados de datastores.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de novembro de 2018, 19:19 UTC
- Hora da edição: 13 de novembro de 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

## Versão da política

Versão da política: v8 (padrão)



A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
```

```
"Action" : [
  "iottwinmaker:GetWorkspace",
  "iottwinmaker:ExecuteQuery"
],
"Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "iottwinmaker:linkedServices" : [
      "IOTSITWISE"
    ]
  }
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy é uma [política AWS gerenciada](#) que: Permite que o serviço de entrega de registros entregue registros ligando para o destino do registro em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de outubro de 2019, 17:31 UTC
- Horário editado: 15 de julho de 2021, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSServiceRoleForMonitronPolicy

AWSServiceRoleForMonitronPolicy é uma [política AWS gerenciada](#) que: Concede permissões ao Amazon Monitron para gerenciar AWS recursos, incluindo a atribuição de usuários de AWS SSO em seu nome.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de dezembro de 2020, 19:06 UTC
- Horário editado: 29 de setembro de 2022, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
```

```
    "sso:AssociateProfile",
    "sso:ListDirectoryAssociations",
    "sso-directory:DescribeUsers",
    "sso-directory:SearchUsers"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForNeptuneGraphPolicy

AWSServiceRoleForNeptuneGraphPolicy é uma [política AWS gerenciada](#) que: Fornece acesso ao Cloudwatch para publicar métricas e registros operacionais e de uso para o Amazon Neptune

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2023, 14:03 UTC
- Horário editado: 29 de novembro de 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GraphLogEvents",
      "Effect" : "Allow",
```

```
"Action" : [
  "logs:CreateLogStream",
  "logs:PutLogEvents",
  "logs:DescribeLogStreams"
],
"Resource" : [
  "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRoleForPrivateMarketplaceAdminPolicy

AWSServiceRoleForPrivateMarketplaceAdminPolicy é uma [política AWS gerenciada](#) que: Fornece permissões para descrever e atualizar recursos do Private Marketplace e descrever AWS Organizations

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 14 de fevereiro de 2024, 22:28 UTC

- Horário editado: 14 de fevereiro de 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
```



```
    "Action" : [
      "aws-marketplace:ListEntities",
      "aws-marketplace:ListChangeSets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:StartChangeSet"
    ],
    "Condition" : {
      "StringEquals" : {
        "catalog:ChangeType" : [
          "AssociateAudience",
          "DisassociateAudience"
        ]
      }
    },
    "Resource" : [
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    ]
  },
  {
    "Sid" : "PrivateMarketplaceOrganizationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganizationalUnit",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListChildren"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSServiceRoleForSMS

`AWSServiceRoleForSMS` é uma [política AWS gerenciada](#) que: fornece acesso aos AWS serviços e recursos necessários para migrar instâncias de serviço, AWS incluindo EC2, S3 e CloudFormation.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 06 de agosto de 2019, 18:39 UTC
- Horário editado: 15 de outubro de 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

### Versão da política

Versão da política: v10 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "cloudformation:CreateChangeSet",
    "cloudformation:CreateStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**",
  "Condition" : {
    "Null" : {
      "cloudformation:ResourceTypes" : "false"
    },
    "ForAllValues:StringEquals" : {
      "cloudformation:ResourceTypes" : [
        "AWS::EC2::Instance",
        "AWS::ApplicationInsights::Application",
        "AWS::ResourceGroups::Group"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:DeleteChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:GetTemplate"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",

```

```

    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*::document/AWS-RunRemoteScript",
    "arn:aws:s3:::sms-app-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CopySnapshot"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CopySnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  }
]
```

```
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DeregisterImage",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
```

```
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "ec2.amazonaws.com"
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "iam:PassedToService" : "cloudformation.amazonaws.com"
    },
    "StringLike" : {
      "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyInstanceAttribute",
    "ec2:StopInstances",
    "ec2:StartInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
```

```

    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*",
      "cloudformation:ListStackResources"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:CreateApplication",
      "applicationinsights:CreateComponent",
      "applicationinsights:UpdateApplication",
      "applicationinsights>DeleteApplication",
      "applicationinsights:UpdateComponentConfiguration",
      "applicationinsights>DeleteComponent"
    ],
    "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:GetGroup",
      "resource-groups:UpdateGroup",
      "resource-groups>DeleteGroup"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  }
}

```



```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRolePolicyForBackupReports

AWSServiceRolePolicyForBackupReports é uma [política AWS gerenciada](#) que: Fornece permissões de AWS Backup para criar relatórios de conformidade em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de agosto de 2021, 21:16 UTC

- Horário editado: 10 de março de 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config>DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config>DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting é uma [política gerenciada pela AWS](#) que: Essa política contém permissões para testar restaurações e limpar recursos criados durante os testes.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 10 de novembro de 2023, 23:37 UTC
- Horário editado: 14 de fevereiro de 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
```

```
"Sid" : "IamPassRole",
"Effect" : "Allow",
"Action" : "iam:PassRole",
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : "backup.amazonaws.com"
  }
}
},
{
  "Sid" : "DescribeActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshotTierStatus",
    "ec2:DescribeTags",
    "ec2:DescribeVolumes",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "fsx:ListTagsForResource",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "rds:DescribeDBClusterAutomatedBackups",
    "rds:ListTagsForResource",
    "redshift:DescribeClusters"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DeleteActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteVolume",
    "ec2:TerminateInstances",
    "elasticfilesystem:DeleteFilesystem",
    "elasticfilesystem:DeleteMountTarget",
    "rds>DeleteDBCluster",
    "rds>DeleteDBInstance",
    "fsx>DeleteFileSystem",
    "fsx>DeleteVolume"
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/awsbackup-restore-test" : "false"
      }
    }
  },
  {
    "Sid" : "DdbDeleteActions",
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:DeleteTable",
      "dynamodb:DescribeTable"
    ],
    "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "RedshiftDeleteActions",
    "Effect" : "Allow",
    "Action" : "redshift:DeleteCluster",
    "Resource" : "arn:aws:redshift:*:*:cluster/awsbackup-restore-test-*"
  },
  {
    "Sid" : "S3DeleteActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration"
    ],
    "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
```

```
    "Sid" : "TimestreamDeleteActions",
    "Effect" : "Allow",
    "Action" : "timestream:DeleteTable",
    "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy é uma [política AWS gerenciada](#) que: Fornece à equipe de resposta a AWS DDoS acesso limitado à sua equipe Conta da AWS para ajudar na mitigação de ataques de DDoS durante um evento de alta gravidade.

### A utilização desta política

Você pode vincular a AWSShieldDRTAccessPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 05 de junho de 2018, 22:29 UTC
- Horário editado: 15 de dezembro de 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSShieldServiceRolePolicy

AWSShieldServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que a AWS Shield acesse AWS recursos em seu nome para fornecer proteção contra DDoS.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de novembro de 2021, 19:17 UTC
- Horário editado: 17 de novembro de 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "AWSShield",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:GetWebACL",
      "wafv2:UpdateWebACL",
      "wafv2:GetWebACLForResource",
      "wafv2:ListResourcesForWebACL",
      "cloudfront:ListDistributions",
      "cloudfront:GetDistribution"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSMForSAPServiceLinkedRolePolicy

AWSSSMForSAPServiceLinkedRolePolicy é uma [política gerenciada pela AWS](#) que: Fornece ao AWS Systems Manager for SAP as permissões necessárias para gerenciar e integrar o software SAP com AWS o.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de novembro de 2022, 01:18 UTC

- Horário editado: 21 de novembro de 2023, 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy é uma [política AWS gerenciada que: Política](#) para função vinculada ao serviço AWSServiceRoleForAmazonSSM\_OpsInsights

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de junho de 2021, 20:12 UTC
- Horário editado: 16 de junho de 2021, 20:12 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator é uma [política AWS gerenciada](#) que: acesso de administrador ao diretório SSO

### A utilização desta política

Você pode vincular a AWSSSODirectoryAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 31 de outubro de 2018, 23:54 UTC
- Horário editado: 20 de outubro de 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Sid" : "AWSSSODirectoryAdministrator",
    "Effect" : "Allow",
    "Action" : [
      "sso-directory:*",
      "identitystore:*",
      "identitystore-auth:*",
      "sso:ListDirectoryAssociations"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly é uma [política AWS gerenciada](#) que: ReadOnly access for SSO Directory

### A utilização desta política

Você pode vincular a AWSSSODirectoryReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 31 de outubro de 2018, 23:49 UTC
- Horário editado: 16 de novembro de 2022, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministrator é uma [política AWS gerenciada](#) que: Fornece acesso dentro do AWS SSO para gerenciar contas AWS mestras e membros e aplicativos em nuvem da Organizations

## A utilização desta política

Você pode vincular a AWSSSOMasterAccountAdministrator aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2018, 20:36 UTC
- Horário editado: 20 de outubro de 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "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"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSSSOManageDelegatedAdministrator",
```

```
"Effect" : "Allow",
"Action" : [
  "organizations:RegisterDelegatedAdministrator",
  "organizations:DeregisterDelegatedAdministrator"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "organizations:ServicePrincipal" : "sso.amazonaws.com"
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator é uma [política AWS gerenciada](#) que: Fornece acesso dentro do AWS SSO para gerenciar contas de membros e aplicativos em nuvem da AWS Organizations

### A utilização desta política

Você pode vincular a AWSSSOMemberAccountAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2018, 20:45 UTC
- Horário editado: 20 de outubro de 2022, 20:32 UTC



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

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "AWSSS0ManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSOReadOnly

AWSSSOReadOnly é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura às configurações de AWS SSO.

### A utilização desta política

Você pode vincular a AWSSSOReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2018, 20:24 UTC

- Horário editado: 22 de agosto de 2022, 17:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSS0ReadOnly`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0ReadOnly",
      "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"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSSOServiceRolePolicy

AWSSSOServiceRolePolicy é uma [política AWS gerenciada](#) que: concede permissões de AWS SSO para gerenciar AWS recursos, incluindo funções, políticas e SAML IdP do IAM em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de dezembro de 2017, 18:36 UTC
- Horário editado: 20 de outubro de 2022, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

### Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam>DeleteRolePermissionsBoundary"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteRole",

```

```
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
  ]
},
{
  "Sid" : "IAMSLRCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus",
    "iam:DeleteRole",
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
  ]
},
{
  "Sid" : "IAMSAMLProviderCreationAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ],
  "Condition" : {
    "StringNotEquals" : {
      "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "IAMSAMLProviderUpdateAction",
  "Effect" : "Allow",
  "Action" : [
    "iam:UpdateSAMLProvider"
  ],
  "Resource" : [
```

```
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ],
},
{
  "Sid" : "IAMSAMLProviderCleanupActions",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteSAMLProvider",
    "iam:GetSAMLProvider"
  ],
  "Resource" : [
    "arn:aws:iam::*:saml-provider/AWSSSO_*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowUnauthAppForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:UnauthorizeApplication"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowDescribeForDirectory",
  "Effect" : "Allow",
  "Action" : [
    "ds:DescribeDirectories",
    "ds:DescribeTrusts"
  ]
},
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
    "Effect" : "Allow",
    "Action" : [
      "identitystore:DescribeUser",
      "identitystore:DescribeGroup",
      "identitystore:ListGroups",
      "identitystore:ListUsers"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess é uma [política AWS gerenciada](#) que: Uma política de acesso para fornecer acesso de usuário/função/etc ao console StepFunctions. AWS Para uma experiência de console completa, além dessa política, um usuário pode precisar da permissão iam:passRole em outras funções do IAM que podem ser assumidas pelo serviço.

## A utilização desta política

Você pode vincular a AWSStepFunctionsConsoleFullAccess aos seus usuários, grupos e perfis.



## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de janeiro de 2017, 21:54 UTC
- Horário editado: 12 de janeiro de 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess` é uma [política AWS gerenciada](#) que: Uma política de acesso para fornecer acesso de usuário/função/etc à API StepFunctions. AWS Para acesso total, além dessa política, o usuário DEVE ter a permissão `iam:passRole` em pelo menos uma função do IAM que possa ser assumida pelo serviço.

### A utilização desta política

Você pode vincular a `AWSStepFunctionsFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de janeiro de 2017, 21:51 UTC
- Horário editado: 11 de janeiro de 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSStepFunctionsReadOnlyAccess

AWSStepFunctionsReadOnlyAccess é uma [política AWS gerenciada que: Uma política](#) de acesso para fornecer a um usuário/função/etc acesso somente de leitura ao serviço StepFunctions. AWS

### A utilização desta política

Você pode vincular a AWSStepFunctionsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de janeiro de 2017, 21:46 UTC
- Horário editado: 10 de novembro de 2017, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSStorageGatewayFullAccess

`AWSStorageGatewayFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Storage Gateway por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a `AWSStorageGatewayFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de setembro de 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "fetchStorageGatewayParams",
    "Effect" : "Allow",
    "Action" : "ssm:GetParameters",
    "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSStorageGatewayReadOnlyAccess

`AWSStorageGatewayReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso ao AWS Storage Gateway por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a `AWSStorageGatewayReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de setembro de 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSStorageGatewayServiceRolePolicy

AWSStorageGatewayServiceRolePolicy é uma [política AWS gerenciada](#) que: função vinculada ao serviço usada pelo AWS Storage Gateway para permitir a integração de outros AWS serviços com o Storage Gateway.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de fevereiro de 2021, 19:03 UTC
- Horário editado: 17 de fevereiro de 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
    "Effect" : "Allow",
    "Action" : [
      "fsx:ListTagsForResource"
    ],
    "Resource" : "arn:aws:fsx:*:*:backup/*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess é uma [política AWS gerenciada](#) que: AWSSupplyChainFederationAdminAccess fornece aos usuários federados da AWS Supply Chain acesso ao aplicativo AWS Supply Chain, incluindo as permissões necessárias para realizar ações dentro do aplicativo AWS Supply Chain. A política fornece permissões administrativas para usuários e grupos do IAM Identity Center e está vinculada a uma função criada pela AWS Supply Chain em seu nome. Você não deve vincular a AWSSupplyChainFederationAdminAccess política a nenhuma outra entidade do IAM.

## Utilização desta política

Você pode vincular a AWSSupplyChainFederationAdminAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 01 de março de 2023, 18:54 UTC
- Hora da edição: 01 de novembro de 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime>DeleteChannelMembership",
        "chime>DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",

```

```
    "chime:SendChannelMessage",
    "chime:UpdateChannelReadMarker",
    "chime:UpdateAppInstanceUser"
  ],
  "Resource" : [
    "arn:aws:chime:*:*:app-instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/SCNInstanceId" : "*"
    }
  }
},
{
  "Sid" : "ChimeChannel",
  "Effect" : "Allow",
  "Action" : [
    "chime:DescribeChannel"
  ],
  "Resource" : [
    "arn:aws:chime:*:*:app-instance/*"
  ]
},
{
  "Sid" : "ChimeMessaging",
  "Effect" : "Allow",
  "Action" : [
    "chime:GetMessagingSessionEndpoint"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMIdentityCenter",
  "Effect" : "Allow",
  "Action" : [
    "sso:GetManagedApplicationInstance",
    "sso:ListDirectoryAssociations",
    "sso:AssociateProfile",
    "sso:DisassociateProfile",
    "sso:ListProfiles",
    "sso:GetProfile",
    "sso:ListProfileAssociations"
  ],
  "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"
  }
}
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSupportAccess

AWSSupportAccess é uma [política AWS gerenciada](#) que: Permite que os usuários acessem o AWS Support Centro.

### A utilização desta política

Você pode vincular a AWSSupportAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSSupportAppFullAccess

AWSSupportAppFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Support Aplicativo e a outros serviços necessários, como AWS Support Service Quotas. Essa política inclui permissões para usar os serviços de suporte para que o usuário possa entrar em contato AWS Support para obter casos de suporte, alterar Service Quotas e criar as funções relevantes vinculadas ao serviço.

## A utilização desta política

Você pode vincular a AWSSupportAppFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de agosto de 2022, 16:53 UTC
- Horário editado: 22 de agosto de 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",

```

```
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
    }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente de leitura ao Amazon AppStream por meio de AWS Support.

### A utilização desta política

Você pode vincular a AWSSupportAppReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de agosto de 2022, 17:01 UTC
- Horário editado: 22 de agosto de 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSSupportPlansFullAccess

AWSSupportPlansFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos planos de suporte.

## A utilização desta política

Você pode vincular a AWSSupportPlansFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de setembro de 2022, 18:19 UTC
- Horário editado: 09 de maio de 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSupportPlansReadOnlyAccess

`AWSSupportPlansReadOnlyAccess` é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao `supportplans`.

### A utilização desta política

Você pode vincular a `AWSSupportPlansReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de setembro de 2022, 18:08 UTC
- Horário editado: 27 de setembro de 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSupportServiceRolePolicy

AWSSupportServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Permite AWS Support acessar AWS recursos para fornecer serviços administrativos, de cobrança e de suporte.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de abril de 2018, 18:04 UTC
- Horário editado: 17 de janeiro de 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

## Versão da política

Versão da política: v34 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
```

```

    "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
    "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
    "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/restapis/*/authorizers",
    "arn:aws:apigateway:*::/restapis/*/authorizers/*",
    "arn:aws:apigateway:*::/restapis/*/deployments",
    "arn:aws:apigateway:*::/restapis/*/deployments/*",
    "arn:aws:apigateway:*::/restapis/*/models",
    "arn:aws:apigateway:*::/restapis/*/models/*",
    "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
    "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/usageplans",
    "arn:aws:apigateway:*::/usageplans/*",
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Sid" : "AWSSupportDeleteRoleAccess",
  "Action" : [
    "iam:DeleteRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam:*::role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
  ]
},
{
  "Sid" : "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:describeWorkspace",
"aps:listRuleGroupsNamespaces",
"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:getSupportedResourceTypes",
"backup:listBackupJobs",
"backup:listBackupPlans",
"backup:listBackupPlanTemplates",
"backup:listBackupPlanVersions",
"backup:listBackupSelections",
"backup:listBackupVaults",
"backup:listCopyJobs",
"backup:listFrameworks",
"backup:listLegalHolds",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
```

```
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup: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: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: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:batchGetProjects",
"codebuild:listBuildBatches",
"codebuild:listBuildBatchesForProject",
"codebuild:listBuilds",
"codebuild:listBuildsForProject",
"codebuild:listCuratedEnvironmentImages",
"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:getLandingZoneStatus",
"controltower:listDirectoryGroups",
"controltower:listGuardrailsForTarget",
"controltower:listGuardrailViolations",
"controltower:listManagedAccounts",
"controltower:listManagedAccountsForGuardrail",
"controltower:listManagedAccountsForParent",
"controltower:listManagedOrganizationalUnits",
"controltower:listManagedOrganizationalUnitsForGuardrail",
"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",
"dln:getLifecyclePolicies",
"dln: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:describeLDAPSettings",
"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",
"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: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:listWorkflowExecutions",
"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: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:describeClusterV2",
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:getBootstrapBrokers",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClusterOperations",
```

```
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"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:getLogDelivery",
"logs:getLogGroupFields",
"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",
"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",
"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:listAllMyDirectoryBuckets",
"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: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: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: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: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"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
}
],
"Version" : "2012-10-17"
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# AWSSystemsManagerAccountDiscoveryServicePolicy

AWSSystemsManagerAccountDiscoveryServicePolicy é uma [política AWS gerenciada](#) que concede permissão ao AWS Systems Manager (SSM) para descobrir Conta da AWS informações.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de outubro de 2019, 17:21 UTC
- Horário editado: 17 de outubro de 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
    "organizations:ListRoots",
    "organizations:ListAccounts",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListChildren",
    "organizations:ListParents",
    "organizations:ListDelegatedServicesForAccount",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy é uma [política AWS gerenciada](#) que: Fornece acesso aos AWS recursos gerenciados ou usados pela estrutura de gerenciamento de alterações do AWS Systems Manager.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de dezembro de 2020, 22:21 UTC
- Horário editado: 07 de dezembro de 2020, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm>DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "sso:ListDirectoryAssociations"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sso-directory:DescribeUsers",
    "sso-directory:IsMemberInGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetGroup",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ssm.amazonaws.com"
      ]
    }
  }
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSSystemsManagerForSAPFullAccess

AWSSystemsManagerForSAPFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço AWS Systems Manager for SAP

## A utilização desta política

Você pode vincular a AWSSystemsManagerForSAPFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de novembro de 2022, 02:11 UTC
- Horário editado: 18 de novembro de 2022, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSystemsManagerForSAPReadOnlyAccess

`AWSSystemsManagerForSAPReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao serviço AWS Systems Manager for SAP

### A utilização desta política

Você pode vincular a `AWSSystemsManagerForSAPReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 17 de novembro de 2022, 02:11 UTC
- Horário editado: 17 de novembro de 2022, 02:11 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSSystemsManagerOpsDataSyncServiceRolePolicy

AWSSystemsManagerOpsDataSyncServiceRolePolicy é uma [política AWS gerenciada](#) que: função do IAM para o SSM Explorer gerenciar operações relacionadas ao OpsData

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de abril de 2021, 20:42 UTC
- Horário editado: 28 de junho de 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
```



```
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateOpsItem"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:AddTagsToResource"
    ],
    "Resource" : "arn:aws:ssm:*:*:opsitem/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:UpdateServiceSetting",
      "ssm:GetServiceSetting"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
      "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "securityhub:GetFindings",
      "securityhub:BatchUpdateFindings"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
      }
    }
  }
},
```

```
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Confidence" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Criticality" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Note.Text" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
    }
  }
},
{
  "Effect" : "Deny",
  "Action" : "securityhub:BatchUpdateFindings",
  "Resource" : "*",
```

```
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/RelatedFindings" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/Types" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
      }
    }
  },
  {
    "Effect" : "Deny",
    "Action" : "securityhub:BatchUpdateFindings",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "securityhub:ASFFSyntaxPath/VerificationState" : false
      }
    }
  }
}
```

```
}  
  }  
] }  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy é uma [política AWS gerenciada](#) que: Essa política concede ao AWS Portal Asset Server as permissões necessárias para a operação normal.

### A utilização desta política

Você pode vincular a AWSThinkboxAssetServerPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2020, 19:18 UTC
- Horário editado: 27 de maio de 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/thinkbox*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-portal-cache*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSThinkboxAWSPortalAdminPolicy

AWSThinkboxAWSPortalAdminPolicy é uma [política AWS gerenciada](#) que: Esta política concede ao software Deadline da AWS Thinkbox acesso total a vários AWS serviços, conforme necessário

para a administração AWS do Portal. Isso inclui acesso para criar tags arbitrárias em vários tipos de recursos do EC2.

## Utilização desta política

Você pode vincular a `AWSThinkboxAWSPortalAdminPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 27 de maio de 2020, 19:41 UTC
- Horário editado: 23 de fevereiro de 2024, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
```

```
"ec2:CreatePlacementGroup",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeAddresses",
"ec2:DescribeFleets",
"ec2:DescribeFleetHistory",
"ec2:DescribeFleetInstances",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeRouteTables",
"ec2:DescribeNatGateways",
"ec2:DescribeTags",
"ec2:DescribeKeyPairs",
"ec2:DescribePlacementGroups",
"ec2:DescribeInstanceTypeOfferings",
"ec2:DescribeRegions",
"ec2:DescribeSpotFleetRequestHistory",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSpotFleetInstances",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotPriceHistory",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeVpcEndpoints",
"ec2:GetConsoleOutput",
"ec2:ImportKeyPair",
"ec2:ReleaseAddress",
"ec2:RequestSpotFleet",
"ec2:CancelSpotFleetRequests",
"ec2:DisassociateAddress",
"ec2>DeleteFleets",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteVpc",
"ec2>DeletePlacementGroup",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteInternetGateway",
"ec2>DeleteSecurityGroup",
```

```

    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteRoute",
    "ec2>DeleteRouteTable",
    "ec2:DisassociateRouteTable",
    "ec2>DeleteSubnet",
    "ec2>DeleteNatGateway",
    "ec2:DetachInternetGateway",
    "ec2:ModifyInstanceAttribute",
    "ec2:ModifyFleet",
    "ec2:ModifySpotFleetRequest",
    "ec2:ModifyVpcAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal2",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal3",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "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"
    ],
    "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:rds-tls-pw*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy é uma [política AWS gerenciada](#) que: Essa política concede à máquina do AWS Portal Gateway as permissões necessárias para a operação normal.

### A utilização desta política

Você pode vincular a AWSThinkboxAWSPortalGatewayPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora de criação: 27 de maio de 2020, 19:05 UTC
- Horário editado: 30 de junho de 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "dynamodb:Scan",
    "Resource" : [
      "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*/gateway_certs/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSThinkboxAWSPortalWorkerPolicy

AWSThinkboxAWSPortalWorkerPolicy é uma [política AWS gerenciada](#) que: Essa política concede aos Deadline Workers no AWS Portal as permissões necessárias para a operação normal.

### A utilização desta política

Você pode vincular a AWSThinkboxAWSPortalWorkerPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2020, 19:15 UTC
- Horário editado: 07 de dezembro de 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:PutObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-portal-cache*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::stack*/gateway_certs/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
```

```
    "logs:DescribeLogStreams",
    "logs:DescribeLogGroups"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:SendMessage",
    "sqs:GetQueueUrl"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWS*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSThinkboxDeadlineResourceTrackerAccessPolicy

AWSThinkboxDeadlineResourceTrackerAccessPolicy é uma [política AWS gerenciada](#) que: Concede as permissões necessárias para a operação do Deadline Resource Tracker da AWS Thinkbox. Isso inclui acesso total a algumas ações do EC2, incluindo DeleteFleets e CancelSpotFleetRequests.

## A utilização desta política

Você pode vincular a AWSThinkboxDeadlineResourceTrackerAccessPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2020, 19:25 UTC
- Horário editado: 27 de maio de 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchWriteItem",
    "dynamodb>DeleteItem",
    "dynamodb:DescribeStream",
    "dynamodb:DescribeTable",
    "dynamodb:GetItem",
    "dynamodb:GetRecords",
    "dynamodb:GetShardIterator",
    "dynamodb:PutItem",
    "dynamodb:Scan",
    "dynamodb:UpdateItem",
    "dynamodb:UpdateTable"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CancelSpotFleetRequests",
    "ec2>DeleteFleets",
    "ec2:DescribeFleetInstances",
    "ec2:DescribeFleets",
    "ec2:DescribeInstances",
    "ec2:DescribeSpotFleetInstances",
    "ec2:DescribeSpotFleetRequests"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RebootInstances",
    "ec2:TerminateInstances"
  ]
}

```

```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "events:PutEvents"
    ],
    "Resource" : [
      "arn:aws:events:*:*:event-bus/default"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource" : [
```



```
    "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes",
    "sqs:ReceiveMessage"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
  ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicy é uma [política AWS gerenciada](#) que: Concede as permissões necessárias para criar, destruir e administrar o Deadline Resource Tracker da AWS Thinkbox.

### A utilização desta política

Você pode vincular a AWSThinkboxDeadlineResourceTrackerAdminPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 27 de maio de 2020, 19:29 UTC
- Horário editado: 22 de junho de 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:UpdateStack",
    "cloudformation:DescribeStacks",
    "cloudformation:UpdateTerminationProtection"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
  ]
},
{
  "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*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchWriteItem",
    "dynamodb:Scan"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "events>DeleteRule",
    "events:DescribeRule",
```

```

    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/DeadlineResourceTracker*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/aws-service-role/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "dynamodb.application-autoscaling.amazonaws.com"
      ]
    }
  }
},
{

```

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

```

    "lambda:CreateEventSourceMapping",
    "lambda>DeleteEventSourceMapping"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "lambda:FunctionArn" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission",
    "lambda:RemovePermission"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
  ],
  "Condition" : {
    "StringLike" : {
      "lambda:Principal" : "events.amazonaws.com"
    }
  }
},
{
  "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*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:/deadline_aws_resource_tracker-*.zip",
      "arn:aws:s3::*:/DeadlineAWSResourceTrackerTemplate-*.yaml"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:CreateQueue",
      "sqs>DeleteQueue",
      "sqs:GetQueueAttributes",
      "sqs:ListQueueTags",
      "sqs:TagQueue",
      "sqs:UntagQueue"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
      "arn:aws:sqs:*:*:DeadlineResourceTracker*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSThinkboxDeadlineSpotEventPluginAdminPolicy

AWSThinkboxDeadlineSpotEventPluginAdminPolicy é uma [política AWS gerenciada](#) que: Concede as permissões necessárias para o plug-in Deadline Spot Event da AWS Thinkbox. Isso inclui permissão para solicitar, modificar e cancelar uma frota spot, bem como permissão limitada do PassRole.

## A utilização desta política

Você pode vincular a AWSThinkboxDeadlineSpotEventPluginAdminPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2020, 19:38 UTC
- Horário editado: 27 de maio de 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
```



```
    "ec2:ModifySpotFleetRequest",
    "ec2:RequestSpotFleet"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam::*:instance-profile/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetUser"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy é uma [política AWS gerenciada](#) que concede as permissões necessárias para uma instância EC2 executando o software AWS Thinkbox Deadline Spot Event Plugin Worker.

### A utilização desta política

Você pode vincular a AWSThinkboxDeadlineSpotEventPluginWorkerPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de maio de 2020, 19:35 UTC
- Horário editado: 07 de dezembro de 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
    "StringEquals" : {
      "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueUrl",
      "sqs:SendMessage"
    ],
    "Resource" : [
      "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSTransferConsoleFullAccess

AWSTransferConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à AWS transferência por meio do AWS Management Console

## A utilização desta política

Você pode vincular a AWSTransferConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de dezembro de 2020, 19:33 UTC
- Horário editado: 14 de dezembro de 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "acm:ListCertificates",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "health:DescribeEventAggregates",
    "iam:GetPolicyVersion",
    "iam:ListPolicies",
    "iam:ListRoles",
    "route53:ListHostedZones",
    "s3:ListAllMyBuckets",
    "transfer:*"
  ],
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTransferFullAccess

AWSTransferFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Serviço AWS de Transferência.

## A utilização desta política

Você pode vincular a AWSTransferFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de dezembro de 2020, 19:37 UTC
- Horário editado: 14 de dezembro de 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
```



```
    "ec2:DescribeAddresses"  
  ],  
  "Resource" : "*" }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTransferLoggingAccess

AWSTransferLoggingAccess é uma [política AWS gerenciada](#) que: Permite AWS transferir acesso total para criar fluxos e grupos de log e colocar eventos de log em sua conta

### A utilização desta política

Você pode vincular a AWSTransferLoggingAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de janeiro de 2019, 15:32 UTC
- Horário editado: 14 de janeiro de 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTransferReadOnlyAccess

AWSTransferReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura aos serviços AWS de transferência.

## A utilização desta política

Você pode vincular a AWSTransferReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de agosto de 2020, 17:54 UTC
- Horário editado: 27 de agosto de 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS Trusted Advisor Priority. Esta política facultativa possibilita ao usuário incluir o Trusted Advisor como um serviço confiável no contexto de AWS Organizações, além de permitir a especificação de contas de administrador delegadas para a Prioridade do Trusted Advisor.

### A utilização desta política

Você pode vincular a AWSTrustedAdvisorPriorityFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de agosto de 2022, 16:08 UTC
- Horário editado: 16 de agosto de 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Action" : [
      "trustedadvisor:DescribeAccount*",
      "trustedadvisor:DescribeOrganization",
      "trustedadvisor:DescribeRisk*",
      "trustedadvisor:DownloadRisk",
      "trustedadvisor:UpdateRiskStatus",
      "trustedadvisor:DescribeNotificationConfigurations",
      "trustedadvisor:UpdateNotificationConfigurations",
      "trustedadvisor>DeleteNotificationConfigurationForDelegatedAdmin",
      "trustedadvisor:SetOrganizationAccess"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators",
      "organizations:EnableAWSServiceAccess",
      "organizations:DisableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "reporting.trustedadvisor.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
    "Condition" : {

```

```
    "StringLike" : {
      "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "arn:aws:organizations::*:*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "reporting.trustedadvisor.amazonaws.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao AWS Trusted Advisor Priority. Isso inclui permissão para visualizar as contas de administrador delegado.

## A utilização desta política

Você pode vincular a `AWSTrustedAdvisorPriorityReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 16 de agosto de 2022, 16:35 UTC
- Horário editado: 16 de agosto de 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : [
        "reporting.trustedadvisor.amazonaws.com"
      ]
    }
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy é uma [política AWS gerenciada](#) que: Service Policy for Trusted Advisor Multi-account Reporting

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.



## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de novembro de 2019, 17:41 UTC
- Horário de edição: 28 de fevereiro de 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Access for the AWS Trusted Advisor Service para ajudar a reduzir custos, aumentar o desempenho e melhorar a segurança do seu AWS ambiente.

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 22 de fevereiro de 2018, 21:24 UTC
- Horário editado: 18 de janeiro de 2024, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

### Versão da política

Versão da política: v12 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "TrustedAdvisorServiceRolePermissions",
    "Effect" : "Allow",
    "Action" : [
      "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",
      "dynamodb:DescribeLimits",
      "dynamodb:DescribeTable",
      "dynamodb:ListTables",
      "ec2:DescribeAddresses",
      "ec2:DescribeReservedInstances",
      "ec2:DescribeInstances",
      "ec2:DescribeVpcs",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeImages",
      "ec2:DescribeVolumes",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeRegions",
      "ec2:DescribeReservedInstancesOfferings",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeVpnGateways",
      "ec2:DescribeLaunchTemplateVersions",
      "ecs:DescribeTaskDefinition",
      "ecs:ListTaskDefinitions",
      "elasticloadbalancing:DescribeAccountLimits",
      "elasticloadbalancing:DescribeInstanceHealth",
      "elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetServerCertificate",
"iam:ListServerCertificates",
"kinesis:DescribeLimits",
"kafka:ListClustersV2",
"kafka:ListNodes",
"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:ListQueues"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: Permite que as notificações AWS do usuário liguem para AWS serviços em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 19 de abril de 2023, 13:28 UTC

- Horário editado: 19 de abril de 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events>DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVendorInsightsAssessorFullAccess

`AWSVendorInsightsAssessorFullAccess` é uma [política AWS gerenciada](#) que: Fornece acesso total para visualização de recursos intitulados do Vendor Insights e gerenciamento de assinaturas do Vendor Insights

### A utilização desta política

Você pode vincular a `AWSVendorInsightsAssessorFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de julho de 2022, 15:05 UTC
- Horário editado: 01 de dezembro de 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```



```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVendorInsightsAssessorReadOnly

`AWSVendorInsightsAssessorReadOnly` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura para visualização dos recursos intitulados do Vendor Insights

### A utilização desta política

Você pode vincular a `AWSVendorInsightsAssessorReadOnly` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de julho de 2022, 15:05 UTC
- Horário editado: 01 de dezembro de 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVendorInsightsVendorFullAccess

AWSVendorInsightsVendorFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total para criar e gerenciar os recursos do Vendor Insights

## A utilização desta política

Você pode vincular a `AWSVendorInsightsVendorFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de julho de 2022, 15:05 UTC
- Horário editado: 19 de outubro de 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",

```

```

    "vendor-insights:DeleteDataSource",
    "vendor-insights:GetDataSource",
    "vendor-insights:ListDataSources",
    "vendor-insights:CreateSecurityProfile",
    "vendor-insights:ListSecurityProfiles",
    "vendor-insights:GetSecurityProfile",
    "vendor-insights:AssociateDataSource",
    "vendor-insights:DisassociateDataSource",
    "vendor-insights:UpdateSecurityProfile",
    "vendor-insights:ActivateSecurityProfile",
    "vendor-insights:DeactivateSecurityProfile",
    "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
    "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
    "vendor-insights:ListSecurityProfileSnapshots",
    "vendor-insights:GetSecurityProfileSnapshot",
    "vendor-insights:TagResource",
    "vendor-insights:UntagResource",
    "vendor-insights:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:AcceptAgreementApprovalRequest",
    "aws-marketplace:RejectAgreementApprovalRequest",
    "aws-marketplace:GetAgreementApprovalRequest",
    "aws-marketplace:ListAgreementApprovalRequests",
    "aws-marketplace:CancelAgreement",
    "aws-marketplace:SearchAgreements"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "artifact:GetReport",
    "artifact:GetReportMetadata",
    "artifact:GetTermForReport",

```

```
    "artifact:ListReports"
  ],
  "Resource" : "arn:aws:artifact:*::report/*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura para visualizar os recursos do Vendor Insights

### A utilização desta política

Você pode vincular a AWSVendorInsightsVendorReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 26 de julho de 2022, 15:05 UTC
- Horário editado: 01 de dezembro de 2022, 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/*SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*:*:report/*"
    }
  ]
}
```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVpcLatticeServiceRolePolicy

AWSVpcLatticeServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o VPC Lattice acesse AWS recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 30 de novembro de 2022, 20:47 UTC
- Horário editado: 30 de novembro de 2022, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVPCS2SVpnServiceRolePolicy

AWSVPCS2SVpnServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite que a Site-to-Site VPN crie e gerencie recursos relacionados às suas conexões VPN.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 06 de agosto de 2019, 14:13 UTC



- Horário editado: 06 de agosto de 2019, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# AWSVPCTransitGatewayServiceRolePolicy

AWSVPCTransitGatewayServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o VPC Transit Gateway crie e gerencie os recursos necessários para seus anexos VPC do Transit Gateway.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2018, 16:21 UTC
- Horário editado: 15 de abril de 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
    ],
    "Resource" : "*",
    "Effect" : "Allow",
    "Sid" : "0"
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSVPCVerifiedAccessServiceRolePolicy

AWSVPCVerifiedAccessServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Política para permitir que o serviço de acesso AWS verificado provisione endpoints em seu nome

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2022, 03:35 UTC
- Horário editado: 17 de novembro de 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ],
  {
```

```

    "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/VerifiedAccessManaged" : "true"
      }
    }
  },
  {
    "Sid" : "VerifiedAccessRoleTaggingActions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  }
]
}

```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWAFConsoleFullAccess

AWSWAFConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao AWS WAF por meio do AWS Management Console. Observe que essa política também concede permissões para listar e atualizar distribuições do Amazon CloudFront, permissões para visualizar balanceadores de carga no Elastic AWS Load Balancing, permissões para visualizar APIs e estágios

REST do Amazon API Gateway, permissões para listar e visualizar métricas do Amazon CloudWatch e permissões para visualizar regiões habilitadas na conta.

## A utilização desta política

Você pode vincular a `AWSWAFConsoleFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de abril de 2020, 18:38 UTC
- Horário editado: 05 de junho de 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWAFConsoleReadOnlyAccess

`AWSWAFConsoleReadOnlyAccess` é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura à AWS WAF por meio de AWS Management Console. Observe que essa política também concede permissões para listar distribuições do Amazon CloudFront, permissões para visualizar balanceadores de carga no Elastic AWS Load Balancing, permissões para visualizar as APIs e estágios REST do Amazon API Gateway, permissões para listar e visualizar métricas do Amazon CloudWatch e permissões para visualizar regiões habilitadas na conta.



## A utilização desta política

Você pode vincular a `AWSWAFConsoleReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de abril de 2020, 18:43 UTC
- Horário editado: 05 de junho de 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWAFFullAccess

AWSWAFFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total às ações do AWS WAF.

## A utilização desta política

Você pode vincular a AWSWAFFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 06 de outubro de 2015, 20:44 UTC
- Horário editado: 05 de junho de 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWAFFReadOnlyAccess

AWSWAFFReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura às ações AWS WAF.

### A utilização desta política

Você pode vincular a AWSWAFFReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de outubro de 2015, 20:43 UTC
- Horário editado: 05 de junho de 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFReadOnlyAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que a WellArchitected acesse AWS serviços e recursos relacionados aos recursos da WellArchitected em nome dos clientes.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de abril de 2023, 18:36 UTC
- Horário editado: 26 de abril de 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```

        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
    ],
    "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
},
{
    "Effect" : "Allow",
    "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog>DeleteAttributeGroup"
    ],
    "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
    ]
}
]
}

```



## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWellArchitectedOrganizationsServiceRolePolicy

AWSWellArchitectedOrganizationsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que a Well-Architected acesse Organizations em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora de criação: 23 de junho de 2022, 17:15 UTC
- Horário editado: 25 de julho de 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAccountsForParent",
      "organizations:ListChildren",
      "organizations:ListParents",
      "organizations:ListRoots"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSWickrFullAccess

AWSWickrFullAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões administrativas completas ao serviço Wickr, incluindo as funções administrativas do Wickr sob o. AWS Management Console

## A utilização desta política

Você pode vincular a AWSWickrFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 20:36 UTC

- Horário editado: 27 de novembro de 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSXrayCrossAccountSharingConfiguration

`AWSXrayCrossAccountSharingConfiguration` é uma [política AWS gerenciada](#) que: Fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento de rastreamentos de X-Ray

## A utilização desta política

Você pode vincular a `AWSXrayCrossAccountSharingConfiguration` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 13:46 UTC
- Horário editado: 27 de novembro de 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "arn:aws:oam:*:*:link/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam:CreateLink",
      "oam:UpdateLink"
    ],
    "Resource" : [
      "arn:aws:oam:*:*:link/*",
      "arn:aws:oam:*:*:sink/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSXRayDaemonWriteAccess

AWSXRayDaemonWriteAccess é uma [política AWS gerenciada](#) que: Permite que o AWS X-Ray Daemon retransmita dados brutos de segmentos de rastreamento para a API do serviço e recupere dados de amostragem (regras, alvos etc.) para serem usados pelo X-Ray SDK.

### Utilização desta política

Você pode vincular a AWSXRayDaemonWriteAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada

- Horário de criação: 28 de agosto de 2018, 23:00 UTC
- Horário editado: 13 de fevereiro de 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## AWSXrayFullAccess

AWSXrayFullAccess é uma [política AWS gerenciada que: política gerenciada](#) de acesso total do AWS X-Ray

### A utilização desta política

Você pode vincular a AWSXrayFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2016, 18:30 UTC
- Horário editado: 01 de dezembro de 2016, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
]
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSXrayReadOnlyAccess

`AWSXrayReadOnlyAccess` é uma [política AWS gerenciada](#) que: AWS X-Ray Read Only Managed Policy

### Utilização desta política

Você pode vincular a `AWSXrayReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 01 de dezembro de 2016, 18:27 UTC
- Horário editado: 14 de fevereiro de 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

### Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

# AWSXrayWriteOnlyAccess

AWSXrayWriteOnlyAccess é uma [política AWS gerenciada](#) que: AWS X-Ray Write Only Managed Policy

## A utilização desta política

Você pode vincular a AWSXrayWriteOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2016, 18:19 UTC
- Horário editado: 28 de agosto de 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## AWSZonalAutoshiftPracticeRunSLRPolicy

AWSZonalAutoshiftPracticeRunSLRPolicy é uma [política AWS gerenciada](#) que: fornece acesso administrativo para execuções práticas de turnos zonais do ARC e acesso aos status de CloudWatch alarme para monitorar as execuções de treinos.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2023, 17:34 UTC
- Horário editado: 29 de novembro de 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# BatchServiceRolePolicy

BatchServiceRolePolicy é uma [política gerenciada pela AWS](#) que: Fornece acesso ao serviço AWS Batch para gerenciar os recursos necessários, incluindo recursos do Amazon EC2 e do Amazon ECS.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 10 de março de 2021, 06:55 UTC
- Horário editado: 05 de dezembro de 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
```

```
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeImages",
    "ec2:DescribeImageAttribute",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSpotFleetInstances",
    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeSpotPriceHistory",
    "ec2:DescribeSpotFleetRequestHistory",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:RequestSpotFleet",
    "autoscaling:DescribeAccountLimits",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeScalingActivities",
    "eks:DescribeCluster",
    "ecs:DescribeClusters",
    "ecs:DescribeContainerInstances",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTasks",
    "ecs:ListClusters",
    "ecs:ListContainerInstances",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "ecs:ListTasks",
    "ecs:DeregisterTaskDefinition",
    "ecs:TagResource",
    "ecs:ListAccountSettings",
    "logs:DescribeLogGroups",
    "iam:GetInstanceProfile",
    "iam:GetRole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSBatchPolicyStatement2",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream"
```

```
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement3",
    "Effect" : "Allow",
    "Action" : [
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement4",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateOrUpdateTags"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSBatchServiceTag" : "false"
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement5",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn",
          "ecs-tasks.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSBatchPolicyStatement6",
    "Effect" : "Allow",
```

```
"Action" : "iam:CreateServiceLinkedRole",
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:AWSServiceName" : [
      "spot.amazonaws.com",
      "spotfleet.amazonaws.com",
      "autoscaling.amazonaws.com",
      "ecs.amazonaws.com"
    ]
  }
},
{
  "Sid" : "AWSBatchPolicyStatement7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSBatchServiceTag" : "false"
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:CancelSpotFleetRequests",
    "ec2:ModifySpotFleetRequest",
    "ec2>DeleteLaunchTemplate"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSBatchServiceTag" : "false"
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement9",
```



```

    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateLaunchConfiguration",
      "autoscaling>DeleteLaunchConfiguration"
    ],
    "Resource" :
"arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement10",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:CreateAutoScalingGroup",
      "autoscaling:UpdateAutoScalingGroup",
      "autoscaling:SetDesiredCapacity",
      "autoscaling>DeleteAutoScalingGroup",
      "autoscaling:SuspendProcesses",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:TerminateInstanceInAutoScalingGroup"
    ],
    "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement11",
    "Effect" : "Allow",
    "Action" : [
      "ecs>DeleteCluster",
      "ecs:DeregisterContainerInstance",
      "ecs:RunTask",
      "ecs:StartTask",
      "ecs:StopTask"
    ],
    "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement12",
    "Effect" : "Allow",
    "Action" : [
      "ecs:RunTask",
      "ecs:StartTask",
      "ecs:StopTask"
    ],
    "Resource" : "arn:aws:ecs:*:*:task-definition/*"
  }
}

```

```
  },
  {
    "Sid" : "AWSBatchPolicyStatement13",
    "Effect" : "Allow",
    "Action" : [
      "ecs:StopTask"
    ],
    "Resource" : "arn:aws:ecs:*:*:task/*/*"
  },
  {
    "Sid" : "AWSBatchPolicyStatement14",
    "Effect" : "Allow",
    "Action" : [
      "ecs:CreateCluster",
      "ecs:RegisterTaskDefinition"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSBatchServiceTag" : "false"
      }
    }
  }
},
{
  "Sid" : "AWSBatchPolicyStatement15",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:ec2:*:*:elastic-gpu/*",
    "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
    "arn:aws:resource-groups:*:*:group/*"
  ]
},
{
```

```
"Sid" : "AWSBatchPolicyStatement16",
"Effect" : "Allow",
"Action" : "ec2:RunInstances",
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSBatchServiceTag" : "false"
  }
}
},
{
  "Sid" : "AWSBatchPolicyStatement17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances",
        "CreateLaunchTemplate",
        "RequestSpotFleet"
      ]
    }
  }
}
]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# Billing

Billing é uma [política gerenciada pela AWS](#) que: Concede permissões para faturamento e gerenciamento de custos. Isso inclui visualizar o uso da conta, modificar orçamentos e métodos de pagamento.

## Utilização desta política

Você pode vincular a Billing aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:33 UTC
- Horário editado: 17 de janeiro de 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

## Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "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",
"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:MakePayment",
" payments:UpdatePaymentPreferences",
" pricing:DescribeServices",
" purchase-orders:AddPurchaseOrder",
" purchase-orders>DeletePurchaseOrder",
" purchase-orders:GetPurchaseOrder",
" purchase-orders:ListPurchaseOrderInvoices",
" purchase-orders:ListPurchaseOrders",
" purchase-orders:ListTagsForResource",
" purchase-orders:ModifyPurchaseOrders",
" purchase-orders:TagResource",
" purchase-orders:UntagResource",
" purchase-orders:UpdatePurchaseOrder",
" purchase-orders:UpdatePurchaseOrderStatus",
" purchase-orders:ViewPurchaseOrders",
" support:CreateCase",
" support:AddAttachmentsToSet",
" sustainability:GetCarbonFootprintSummary",
" tax:BatchPutTaxRegistration",
" tax>DeleteTaxRegistration",
" tax:GetExemptions",
" tax:GetTaxInheritance",
" tax:GetTaxInterview",
" tax:GetTaxRegistration",
" tax:GetTaxRegistrationDocument",
" tax:ListTaxRegistrations",
```

```
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CertificateManagerServiceRolePolicy

CertificateManagerServiceRolePolicy é uma [política AWS gerenciada do que: Política de função de serviço do Amazon Certificate Manager](#)

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 25 de junho de 2020, 17:56 UTC
- Horário editado: 25 de junho de 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ClientVPNServiceConnectionsRolePolicy

ClientVPNServiceConnectionsRolePolicy é uma [política AWS gerenciada](#) que: Política para permitir que o AWS Client VPN gerencie suas conexões de endpoint do Client VPN.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.



## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de agosto de 2020, 19:48 UTC
- Horário editado: 12 de agosto de 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# ClientVPNServiceRolePolicy

ClientVPNServiceRolePolicy é uma [política AWS gerenciada](#) que: Política para permitir que o AWS Client VPN gere seus endpoints do Client VPN.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário da criação: 10 de dezembro de 2018, 21:20 UTC
- Horário editado: 12 de agosto de 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
    "ec2:DeleteNetworkInterface",
    "ec2:DescribeAccountAttributes",
    "ds:AuthorizeApplication",
    "ds:DescribeDirectories",
    "ds:GetDirectoryLimits",
    "ds:UnauthorizeApplication",
    "logs:DescribeLogStreams",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogGroups",
    "acm:GetCertificate",
    "acm:DescribeCertificate",
    "iam:GetSAMLProvider",
    "lambda:GetFunctionConfiguration"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy é uma [política AWS gerenciada](#) que: Função de serviço para CloudFormation StackSets (conta principal da organização)

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 10 de dezembro de 2019, 00:20 UTC

- Horário editado: 10 de dezembro de 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# CloudFormationStackSetsOrgMemberServiceRolePolicy

CloudFormationStackSetsOrgMemberServiceRolePolicy é uma [política AWS gerenciada](#) que: Função de serviço para CloudFormation StackSets (conta de membro da organização)

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de dezembro de 2019, 23:52 UTC
- Horário editado: 09 de dezembro de 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
    "arn:aws:iam::*:role/stacksets-exec-*"
  ],
},
{
  "Action" : [
    "iam:DetachRolePolicy",
    "iam:AttachRolePolicy"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam::*:role/stacksets-exec-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudFrontFullAccess

CloudFrontFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao CloudFront console, além da capacidade de listar buckets do Amazon S3 por meio do. AWS Management Console

### Utilização desta política

Você pode vincular a CloudFrontFullAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS

- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 04 de janeiro de 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudFrontReadOnlyAccess

CloudFrontReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso às informações CloudFront de configuração de distribuição e lista distribuições por meio do AWS Management Console.

## Utilização desta política

Você pode vincular a CloudFrontReadOnlyAccess aos seus usuários, grupos e perfis.



## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 04 de janeiro de 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

## Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

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

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudHSMServiceRolePolicy

CloudHSMServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso aos AWS recursos usados ou gerenciados pelo CloudHSM

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 06 de novembro de 2017, 19:12 UTC
- Horário editado: 06 de novembro de 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudSearchFullAccess

CloudSearchFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço de configuração do Amazon CloudSearch.

### A utilização desta política

Você pode vincular a CloudSearchFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC

- Horário editado: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudSearchReadOnlyAccess

`CloudSearchReadOnlyAccess` é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao serviço de configuração do Amazon CloudSearch.

## A utilização desta política

Você pode vincular a `CloudSearchReadOnlyAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 06 de fevereiro de 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudTrailServiceRolePolicy

CloudTrailServiceRolePolicy é uma [política AWS gerenciada](#) que: Política de permissão para CloudTrail ServiceLinkedRole

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de outubro de 2018, 21:21 UTC
- Horário editado: 27 de novembro de 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

### Documento da política JSON

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

```

    "Action" : [
      "cloudtrail:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AwsOrgsAccess",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AwsOrgsDelegatedAdminAccess",
    "Effect" : "Allow",
    "Action" : "organizations:ListDelegatedAdministrators",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : [
          "cloudtrail.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "DeleteTableAccess",
    "Effect" : "Allow",
    "Action" : "glue:DeleteTable",
    "Resource" : [
      "arn:*:glue:*:*:catalog",
      "arn:*:glue:*:*:database/aws:cloudtrail",
      "arn:*:glue:*:*:table/aws:cloudtrail/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }

```

```
    }
  },
  {
    "Sid" : "DeregisterResourceAccess",
    "Effect" : "Allow",
    "Action" : "lakeformation:DeregisterResource",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatch-CrossAccountAccess

CloudWatch-CrossAccountAccess é uma [política AWS gerenciada](#) que: Permite que o CloudWatch assuma funções de CloudWatch-CrossAccountSharing em contas remotas em nome da conta atual, a fim de exibir dados entre contas e regiões

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de julho de 2019, 09:59 UTC
- Horário editado: 23 de julho de 2019, 09:59 UTC



- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchActionsEC2Access

CloudWatchActionsEC2Access é uma [política AWS gerenciada](#) que: Fornece acesso somente leitura aos alarmes e às métricas do CloudWatch, bem como aos metadados do EC2. Fornece acesso para parar, encerrar e reinicializar instâncias do EC2.

## A utilização desta política

Você pode vincular a `CloudWatchActionsEC2Access` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de julho de 2015, 00:00 UTC
- Horário editado: 07 de julho de 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchAgentAdminPolicy

CloudWatchAgentAdminPolicy é uma [política AWS gerenciada](#) que: É necessário ter todas as permissões de uso AmazonCloudWatchAgent.

### Utilização desta política

Você pode vincular a CloudWatchAgentAdminPolicy aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 07 de março de 2018, 00:52 UTC
- Horário editado: 05 de fevereiro de 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Sid" : "CWACloudWatchPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData",
      "ec2:DescribeTags",
      "logs:PutLogEvents",
      "logs:PutRetentionPolicy",
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups",
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingRules",
      "xray:GetSamplingTargets",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CWASSMPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameter",
      "ssm:PutParameter"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy é uma [política AWS gerenciada](#) que: Permissões necessárias para uso AmazonCloudWatchAgent em servidores

## Utilização desta política

Você pode vincular a CloudWatchAgentServerPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 07 de março de 2018, 01:06 UTC
- Horário editado: 06 de fevereiro de 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
```

```
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "xray:PutTraceSegments",
    "xray:PutTelemetryRecords",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetSamplingStatisticSummaries"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CWASSMServerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchApplicationInsightsFullAccess

CloudWatchApplicationInsightsFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao CloudWatch Application Insights e às dependências necessárias.

### A utilização desta política

Você pode vincular a CloudWatchApplicationInsightsFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de novembro de 2020, 18:44 UTC
- Horário editado: 25 de janeiro de 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
```

```
    "sns:ListTopics",
    "states:ListStateMachines",
    "apigateway:GET",
    "ecs:ListClusters",
    "ecs:DescribeTaskDefinition",
    "ecs:ListServices",
    "ecs:ListTasks",
    "eks:ListClusters",
    "eks:ListNodegroups",
    "fsx:DescribeFileSystems",
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "application-insights.amazonaws.com"
    }
  }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# CloudWatchApplicationInsightsReadOnlyAccess

CloudWatchApplicationInsightsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao CloudWatch Application Insights.

## A utilização desta política

Você pode vincular a CloudWatchApplicationInsightsReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de novembro de 2020, 18:48 UTC
- Horário editado: 24 de novembro de 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudwatchApplicationInsightsServiceLinkedRolePolicy

CloudwatchApplicationInsightsServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: Cloudwatch Application Insights Service Linked Role Policy

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 01 de dezembro de 2018, 16:22 UTC
- Horário editado: 11 de maio de 2023, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

### Versão da política

Versão da política: v24 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchApplicationSignalsServiceRolePolicy

CloudWatchApplicationSignalsServiceRolePolicy é uma [política AWS gerenciada](#) que: A política concede permissão ao CloudWatch Application Signals para coletar dados de monitoramento e marcação de outros AWS serviços relevantes.

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de novembro de 2023, 18:09 UTC
- Horário editado: 07 de março de 2024, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid" : "CWLogsPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery",
      "logs:GetQueryResults"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "CWMetricsPermission",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
```

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## CloudWatchAutomaticDashboardsAccess

CloudWatchAutomaticDashboardsAccess é uma [política AWS gerenciada](#) que: Fornece acesso às APIs que não são do CloudWatch usadas para exibir painéis automáticos do CloudWatch, incluindo o conteúdo de objetos, como funções Lambda

### A utilização desta política

Você pode vincular a CloudWatchAutomaticDashboardsAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 23 de julho de 2019, 10:01 UTC
- Horário editado: 20 de abril de 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
    }
  ],
}
```



```
    "Resource" : "*"
  },
  {
    "Action" : [
      "apigateway:GET"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:apigateway:*::/restapis*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchCrossAccountSharingConfiguration

CloudWatchCrossAccountSharingConfiguration é uma [política AWS gerenciada](#) que: Fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento dos recursos do CloudWatch

### A utilização desta política

Você pode vincular a CloudWatchCrossAccountSharingConfiguration aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 14:01 UTC
- Horário editado: 27 de novembro de 2022, 14:01 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam>DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchEventsBuiltInTargetExecutionAccess

CloudWatchEventsBuiltInTargetExecutionAccess é uma [política AWS gerenciada](#) que: Permite que alvos incorporados no Amazon CloudWatch Events executem ações do EC2 em seu nome.

### A utilização desta política

Você pode vincular a CloudWatchEventsBuiltInTargetExecutionAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 14 de janeiro de 2016, 18:35 UTC
- Horário editado: 14 de janeiro de 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchEventsFullAccess

CloudWatchEventsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon CloudWatch Events.

## A utilização desta política

Você pode vincular a `CloudWatchEventsFullAccess` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de janeiro de 2016, 18:37 UTC
- Horário editado: 01 de dezembro de 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```

    "Resource" : "arn:aws:iam::*:role/aws-service-role/
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"
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchEventsInvocationAccess

CloudWatchEventsInvocationAccess é uma [política AWS gerenciada](#) que: Permite que o Amazon CloudWatch Events retransmita eventos para os streams no AWS Kinesis Streams em sua conta.

### A utilização desta política

Você pode vincular a CloudWatchEventsInvocationAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço

- Horário de criação: 14 de janeiro de 2016, 18:36 UTC
- Horário editado: 14 de janeiro de 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# CloudWatchEventsReadOnlyAccess

CloudWatchEventsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon CloudWatch Events.

## A utilização desta política

Você pode vincular a CloudWatchEventsReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 14 de janeiro de 2016, 18:27 UTC
- Horário editado: 01 de dezembro de 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
```

```

    "events:TestEventPattern",
    "events:DescribeArchive",
    "events:ListArchives",
    "events:DescribeReplay",
    "events:ListReplays",
    "events:DescribeConnection",
    "events:ListConnections",
    "events:DescribeApiDestination",
    "events:ListApiDestinations",
    "events:DescribeEndpoint",
    "events:ListEndpoints",
    "schemas:DescribeCodeBinding",
    "schemas:DescribeDiscoverer",
    "schemas:DescribeRegistry",
    "schemas:DescribeSchema",
    "schemas:ExportSchema",
    "schemas:GetCodeBindingSource",
    "schemas:GetDiscoveredSchema",
    "schemas:GetResourcePolicy",
    "schemas:ListDiscoverers",
    "schemas:ListRegistries",
    "schemas:ListSchemas",
    "schemas:ListSchemaVersions",
    "schemas:ListTagsForResource",
    "schemas:SearchSchemas",
    "scheduler:GetSchedule",
    "scheduler:GetScheduleGroup",
    "scheduler:ListSchedules",
    "scheduler:ListScheduleGroups",
    "scheduler:ListTagsForResource",
    "pipes:DescribePipe",
    "pipes:ListPipes",
    "pipes:ListTagsForResource"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchEventsServiceRolePolicy

CloudWatchEventsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o AWS CloudWatch execute ações em seu nome configuradas por meio de alarmes e eventos.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de novembro de 2017, 00:42 UTC
- Horário editado: 17 de novembro de 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "cloudwatch:DescribeAlarms",
  "ec2:DescribeInstanceStatus",
  "ec2:DescribeInstances",
  "ec2:DescribeSnapshots",
  "ec2:DescribeVolumeStatus",
  "ec2:DescribeVolumes",
  "ec2:RebootInstances",
  "ec2:StopInstances",
  "ec2:TerminateInstances",
  "ec2:CreateSnapshot"
],
"Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchFullAccess

CloudWatchFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao CloudWatch.

### A utilização desta política

Você pode vincular a CloudWatchFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 27 de novembro de 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
    }
  ]
}
```

```
    "Resource" : "arn:aws:oam:*:*:sink/*"  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchFullAccessV2

CloudWatchFullAccessV2 é uma [política AWS gerenciada](#) que: Fornece acesso total CloudWatch a.

### Utilização desta política

Você pode vincular a CloudWatchFullAccessV2 aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 01 de agosto de 2023, 11:32 UTC
- Horário editado: 05 de dezembro de 2023, 19:36 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "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/*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchInternetMonitorServiceRolePolicy

CloudWatchInternetMonitorServiceRolePolicy é uma [política AWS gerenciada](#) que: permite que o Internet Monitor acesse os recursos do EC2, do Workspaces e do CloudFront, além de outros serviços necessários em seu nome.



## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 27 de novembro de 2022, 17:46 UTC
- Horário editado: 20 de julho de 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
    "Action" : "logs:CreateLogGroup",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/InternetMonitor"
      }
    },
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy é uma [política AWS gerenciada](#) que: Política necessária para a extensão Lambda Insights

### A utilização desta política

Você pode vincular a CloudWatchLambdaInsightsExecutionRolePolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de outubro de 2020, 19:27 UTC
- Horário editado: 07 de outubro de 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchLogsCrossAccountSharingConfiguration

CloudWatchLogsCrossAccountSharingConfiguration é uma [política AWS gerenciada](#) que: Fornece recursos para gerenciar links do Observability Access Manager e estabelecer o compartilhamento dos recursos do CloudWatch Logs

### A utilização desta política

Você pode vincular a CloudWatchLogsCrossAccountSharingConfiguration aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 13:55 UTC
- Horário editado: 27 de novembro de 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:Link",
      "oam:ListLinks"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam>DeleteLink",
      "oam:GetLink",
      "oam:TagResource"
    ],
    "Resource" : "arn:aws:oam:*:*:link/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "oam>CreateLink",
      "oam:UpdateLink"
    ],
    "Resource" : [
      "arn:aws:oam:*:*:link/*",
      "arn:aws:oam:*:*:sink/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# CloudWatchLogsFullAccess

CloudWatchLogsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total aos CloudWatch registros

## Utilização desta política

Você pode vincular a CloudWatchLogsFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 26 de novembro de 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchLogsReadOnlyAccess

CloudWatchLogsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura aos CloudWatch registros

### Utilização desta política

Você pode vincular a CloudWatchLogsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 26 de novembro de 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchNetworkMonitorServiceRolePolicy

CloudWatchNetworkMonitorServiceRolePolicy é uma [política AWS gerenciada](#) que: permite que o CloudWatch Network Monitor acesse e gerencie recursos do EC2 e VPC, publique dados CloudWatch e acesse outros serviços necessários em seu nome.



## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 21 de dezembro de 2023, 18:53 UTC
- Horário editado: 21 de dezembro de 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

```
"Sid" : "DescribeAny",
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeNetworkInterfaceAttribute",
  "ec2:DescribeVpcs",
  "ec2:DescribeNetworkInterfacePermissions",
  "ec2:DescribeSubnets",
  "ec2:DescribeSecurityGroups"
],
"Resource" : "*"
},
{
  "Sid" : "DeleteModifyEc2Resources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
    }
  }
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# CloudWatchReadOnlyAccess

CloudWatchReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente para CloudWatch leitura a.

## Utilização desta política

Você pode vincular a CloudWatchReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 05 de dezembro de 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "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/*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchSyntheticsFullAccess

CloudWatchSyntheticsFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao CloudWatch Synthetics.

### A utilização desta política

Você pode vincular a CloudWatchSyntheticsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 25 de novembro de 2019, 17:39 UTC
- Horário editado: 06 de maio de 2022, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

### Versão da política

Versão da política: v9 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutEncryptionConfiguration"
  ],
  "Resource" : [
    "arn:aws:s3:::cw-syn-results-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles",
    "s3:ListAllMyBuckets",
    "xray:GetTraceSummaries",
    "xray:BatchGetTraces",
    "apigateway:GET"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3:::cw-syn-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
},
{
```

```
"Effect" : "Allow",
"Action" : [
  "iam:PassRole"
],
"Resource" : [
  "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "lambda.amazonaws.com",
      "synthetics.amazonaws.com"
    ]
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch::*:alarm:Synthetics-*"
  ]
},
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "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"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CloudWatchSyntheticsReadOnlyAccess

CloudWatchSyntheticsReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao CloudWatch Synthetics.

### A utilização desta política

Você pode vincular a CloudWatchSyntheticsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário da criação: 25 de novembro de 2019, 17:45 UTC
- Horário editado: 06 de março de 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComprehendDataAccessRolePolicy

ComprehendDataAccessRolePolicy é uma [política AWS gerenciada](#) que: função de serviço Policy for AWS Comprehend que permite acesso aos recursos do S3 para acesso aos dados

## A utilização desta política

Você pode vincular a `ComprehendDataAccessRolePolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de março de 2019, 22:28 UTC
- Horário editado: 06 de março de 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*Comprehend*",
      "arn:aws:s3::*comprehend*"
    ]
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComprehendFullAccess

ComprehendFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Comprehend.

### A utilização desta política

Você pode vincular a ComprehendFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 18:08 UTC
- Horário editado: 05 de dezembro de 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "comprehend:*",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComprehendMedicalFullAccess

ComprehendMedicalFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Comprehend Medical

### A utilização desta política

Você pode vincular a ComprehendMedicalFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 17:55 UTC
- Horário editado: 27 de novembro de 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComprehendReadOnly

ComprehendReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon Comprehend.

## A utilização desta política

Você pode vincular a ComprehendReadOnly aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 18:10 UTC
- Horário editado: 26 de abril de 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

## Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",

```



```

    "comprehend:DescribeEntitiesDetectionJob",
    "comprehend:ListEntitiesDetectionJobs",
    "comprehend:DescribeKeyPhrasesDetectionJob",
    "comprehend:ListKeyPhrasesDetectionJobs",
    "comprehend:DescribePiiEntitiesDetectionJob",
    "comprehend:ListPiiEntitiesDetectionJobs",
    "comprehend:DescribeSentimentDetectionJob",
    "comprehend:DescribeTargetedSentimentDetectionJob",
    "comprehend:ListSentimentDetectionJobs",
    "comprehend:ListTargetedSentimentDetectionJobs",
    "comprehend:DescribeDocumentClassifier",
    "comprehend:ListDocumentClassifiers",
    "comprehend:DescribeDocumentClassificationJob",
    "comprehend:ListDocumentClassificationJobs",
    "comprehend:DescribeEntityRecognizer",
    "comprehend:ListEntityRecognizers",
    "comprehend:ListTagsForResource",
    "comprehend:DescribeEndpoint",
    "comprehend:ListEndpoints",
    "comprehend:ListDocumentClassifierSummaries",
    "comprehend:ListEntityRecognizerSummaries",
    "comprehend:DescribeResourcePolicy"
  ],
  "Resource" : "*"
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComputeOptimizerReadOnlyAccess

ComputeOptimizerReadOnlyAccess é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura ao ComputeOptimizer.

## A utilização desta política

Você pode vincular a `ComputeOptimizerReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 07 de março de 2020, 00:11 UTC
- Horário editado: 28 de agosto de 2023, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ComputeOptimizerServiceRolePolicy

ComputeOptimizerServiceRolePolicy é uma [política gerenciada da AWS](#) que: permite que o ComputeOptimizer chame os serviços da AWS e colete detalhes do workload em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 03 de dezembro de 2019, 08:45 UTC
- Horário editado: 13 de junho de 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  {
```

```
    "Sid" : "CloudWatchAccess",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AutoScalingAccess",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeAutoScalingGroups"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "Ec2Access",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeVolumes"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ConfigConformsServiceRolePolicy

ConfigConformsServiceRolePolicy é uma [política AWS gerenciada](#) que: Política necessária para que o AWSConfig crie pacotes de conformidade

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 25 de julho de 2019, 21:38 UTC
- Horário editado: 12 de janeiro de 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config>DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
    }
  ]
}
```

```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config:DescribeRemediationConfigurations",
      "config>DeleteRemediationConfiguration",
      "config:PutRemediationConfigurations"
    ],
    "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-remediation-configuration/config-conforms.amazonaws.com*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/config-conforms.amazonaws.com/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam:*:*:role/aws-service-role/remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "remediation.config.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {

```

```
    "StringEquals" : {
      "iam:PassedToService" : "ssm.amazonaws.com"
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:GetObject",
      "s3:GetBucketAcl"
    ],
    "Resource" : "arn:aws:s3:::awsconfigconforms*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStackResources",
      "cloudformation:DescribeStacks",
      "cloudformation:GetStackPolicy",
      "cloudformation:SetStackPolicy",
      "cloudformation:UpdateStack",
      "cloudformation:UpdateTerminationProtection",
      "cloudformation:ValidateTemplate",
      "cloudformation:ListStackResources"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
```



```
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/Config"
    }
  }
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CostOptimizationHubAdminAccess

CostOptimizationHubAdminAccess é uma [política AWS gerenciada](#) que: Essa política gerenciada fornece acesso administrativo ao Cost Optimization Hub.

### Utilização desta política

Você pode vincular a CostOptimizationHubAdminAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 19 de dezembro de 2023, 00:03 UTC
- Horário editado: 19 de dezembro de 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
```

```
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "cost-optimization-hub.bcm.amazonaws.com"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CostOptimizationHubReadOnlyAccess

CostOptimizationHubReadOnlyAccess é uma [política AWS gerenciada](#) que: Essa política gerenciada fornece acesso somente para leitura ao Cost Optimization Hub.

### Utilização desta política

Você pode vincular a CostOptimizationHubReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 13 de dezembro de 2023, 18:04 UTC
- Horário editado: 13 de dezembro de 2023, 18:04 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# CostOptimizationHubServiceRolePolicy

CostOptimizationHubServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Cost Optimization Hub recupere informações da organização e colete dados e metadados relacionados à otimização.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 26 de novembro de 2023, 08:03 UTC
- Horário editado: 26 de novembro de 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## CustomerProfilesServiceLinkedRolePolicy

CustomerProfilesServiceLinkedRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Amazon Connect Customer Profiles acesse AWS serviços e recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 07 de março de 2023, 22:56 UTC
- Horário editado: 07 de março de 2023, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/`  
`CustomerProfilesServiceLinkedRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam>DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## DatabaseAdministrator

DatabaseAdministrator é uma [política AWS gerenciada](#) que: Concede permissões de acesso total aos AWS serviços e ações necessários para instalar e configurar serviços AWS de banco de dados.

### A utilização desta política

Você pode vincular a DatabaseAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:25 UTC
- Horário editado: 08 de janeiro de 2019, 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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



```
"Action" : [  
  "cloudwatch:DeleteAlarms",  
  "cloudwatch:Describe*",  
  "cloudwatch:DisableAlarmActions",  
  "cloudwatch:EnableAlarmActions",  
  "cloudwatch:Get*",  
  "cloudwatch:List*",  
  "cloudwatch:PutMetricAlarm",  
  "datapipeline:ActivatePipeline",  
  "datapipeline:CreatePipeline",  
  "datapipeline>DeletePipeline",  
  "datapipeline:DescribeObjects",  
  "datapipeline:DescribePipelines",  
  "datapipeline:GetPipelineDefinition",  
  "datapipeline:ListPipelines",  
  "datapipeline:PutPipelineDefinition",  
  "datapipeline:QueryObjects",  
  "dynamodb:*",  
  "ec2:DescribeAccountAttributes",  
  "ec2:DescribeAddresses",  
  "ec2:DescribeAvailabilityZones",  
  "ec2:DescribeInternetGateways",  
  "ec2:DescribeSecurityGroups",  
  "ec2:DescribeSubnets",  
  "ec2:DescribeVpcs",  
  "elasticache:*",  
  "iam:ListRoles",  
  "iam:GetRole",  
  "kms:ListKeys",  
  "lambda:CreateEventSourceMapping",  
  "lambda:CreateFunction",  
  "lambda>DeleteEventSourceMapping",  
  "lambda>DeleteFunction",  
  "lambda:GetFunctionConfiguration",  
  "lambda:ListEventSourceMappings",  
  "lambda:ListFunctions",  
  "logs:DescribeLogGroups",  
  "logs:DescribeLogStreams",  
  "logs:FilterLogEvents",  
  "logs:GetLogEvents",  
  "logs:Create*",  
  "logs:PutLogEvents",  
  "logs:PutMetricFilter",  
  "rds:*",
```

```

    "redshift:*",
    "s3:CreateBucket",
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:Get*",
    "sns:List*",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutBucketWebsite",
    "s3:PutLifecycleConfiguration",
    "s3:PutReplicationConfiguration",
    "s3:PutObject*",
    "s3:Replicate*",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/rds-monitoring-role",
    "arn:aws:iam::*:role/rdbms-lambda-access",
    "arn:aws:iam::*:role/lambda_exec_role",
    "arn:aws:iam::*:role/lambda-dynamodb-*",
    "arn:aws:iam::*:role/lambda-vpc-execution-role",

```

```
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
    ]
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## DataScientist

DataScientist é uma [política AWS gerenciada](#) que: Concede permissões aos serviços AWS de análise de dados.

### A utilização desta política

Você pode vincular a DataScientist aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:28 UTC
- Horário editado: 03 de dezembro de 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

### Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
```

```
    "lambda:Delete*",
    "lambda:Get*",
    "lambda:InvokeFunction",
    "lambda:PublishVersion",
    "lambda:Update*",
    "lambda:List*",
    "machinelearning:*",
    "sdb:*",
    "rds:*",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "redshift:*",
    "s3:CreateBucket",
    "sns:CreateTopic",
    "sns:Get*",
    "sns:List*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:Abort*",
    "s3:DeleteObject",
    "s3:Get*",
    "s3:List*",
    "s3:PutAccelerateConfiguration",
    "s3:PutBucketCors",
    "s3:PutBucketLogging",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:Replicate*",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
```

```

    "Action" : [
      "ec2:RunInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DataPipelineDefaultRole",
      "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
      "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "arn:aws:iam::*:role/EMR_DefaultRole",
      "arn:aws:iam::*:role/kinesis-*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:*"
    ],
    "NotResource" : [
      "arn:aws:sagemaker::*:domain/*",
      "arn:aws:sagemaker::*:user-profile/*",
      "arn:aws:sagemaker::*:app/*",
      "arn:aws:sagemaker::*:flow-definition*"
    ]
  }

```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# DAXServiceRolePolicy

DAXServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa política permite que o DAX crie e gerencie interface de rede, grupo de segurança, sub-rede e Vpc em nome do cliente

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de março de 2018, 17:51 UTC
- Horário editado: 05 de março de 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
```



```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permissões necessárias para oferecer suporte ao Amazon CloudWatch Contributor Insights para o Amazon DynamoDB.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de novembro de 2019, 21:13 UTC
- Horário editado: 15 de novembro de 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy é uma [política AWS gerenciada](#) que: Fornece acesso do AWS DynamoDB ao KinesisDataStreams

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora de criação: 12 de novembro de 2020, 00:43 UTC
- Horário editado: 12 de novembro de 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kinesis:PutRecord",
      "kinesis:PutRecords",
      "kinesis:DescribeStream"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy é uma [política gerenciada pela AWS](#): Permissões exigidas pelo DynamoDB para replicação de dados entre regiões

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 09 de novembro de 2017, 23:55 UTC
- Horário editado: 08 de janeiro de 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb>DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "dynamodb.application-autoscaling.amazonaws.com"
      ]
    }
  }
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy é uma [política AWS gerenciada](#) que: A política concede ao ec2fastlaunch a preparação e o gerenciamento de instantâneos pré-provisionados na conta do cliente e a publicação de métricas relacionadas.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora de criação: 10 de janeiro de 2022, 13:08 UTC
- Horário editado: 10 de janeiro de 2022, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "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:DescribeInstanceState",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypeOfferings",
      "ec2:DescribeLaunchTemplateVersions",
      "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/EC2"
      }
    }
  }
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2FleetTimeShiftableServiceRolePolicy

EC2FleetTimeShiftableServiceRolePolicy é uma [política AWS gerenciada](#) que: Política que concede permissões à EC2 Fleet para iniciar instâncias no futuro.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 23 de dezembro de 2019, 19:47 UTC
- Horário editado: 23 de dezembro de 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeImages",
  "ec2:DescribeSubnets",
  "ec2:DescribeInstances",
  "ec2:RunInstances",
  "ec2:CreateFleet"
],
"Resource" : [
  "*"
]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:spot-instances-request/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
}
```

```
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## Ec2ImageBuilderCrossAccountDistributionAccess

Ec2ImageBuilderCrossAccountDistributionAccess é uma [política AWS gerenciada](#) que: Permissões necessárias pelo EC2 Image Builder para realizar uma distribuição entre contas.

### A utilização desta política

Você pode vincular a Ec2ImageBuilderCrossAccountDistributionAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de setembro de 2020, 19:22 UTC
- Horário editado: 30 de setembro de 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2ImageBuilderLifecycleExecutionPolicy

EC2ImageBuilderLifecycleExecutionPolicy é uma [política AWS gerenciada](#) que: A ImageBuilderLifecycleExecutionPolicy política do EC2 concede permissões para o Image Builder realizar ações como descontinuar ou excluir recursos de imagem do Image Builder e seus recursos

subjacentes (AMIs, instantâneos) para dar suporte a regras automatizadas para tarefas de gerenciamento do ciclo de vida da imagem.

## Utilização desta política

Você pode vincular a `EC2ImageBuilderLifecycleExecutionPolicy` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 16 de novembro de 2023, 23:23 UTC
- Horário editado: 16 de novembro de 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ]
    }
  ],
}
```

```
"Resource" : "arn:aws:ec2:*::image/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
  }
},
{
  "Sid" : "EC2DeleteSnapshotPermission",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteSnapshot",
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
    }
  }
},
{
  "Sid" : "EC2TagsPermission",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteTags",
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*::snapshot/*",
    "arn:aws:ec2:*::image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
      "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "DeprecatedBy"
    }
  }
},
{
  "Sid" : "ECRIImagePermission",
  "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" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2InstanceConnect

EC2InstanceConnect é uma [política AWS gerenciada](#) que: permite que os clientes liguem para o EC2 Instance Connect para publicar chaves efêmeras em suas instâncias do EC2 e se conectem via ssh ou pela CLI do EC2 Instance Connect.

## A utilização desta política

Você pode vincular a EC2InstanceConnect aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de junho de 2019, 18:53 UTC
- Horário editado: 27 de junho de 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## Ec2InstanceConnectEndpoint

Ec2InstanceConnectEndpoint é uma [política AWS gerenciada que: política](#) de endpoint do EC2 Instance Connect para gerenciar endpoints do EC2 Instance Connect criados pelo cliente

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de janeiro de 2023, 20:19 UTC
- Horário editado: 24 de janeiro de 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
    },
  ],
}
```

```

    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:subnet/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "InstanceConnectEndpointId"
        ]
      },
      "Null" : {
        "aws:RequestTag/InstanceConnectEndpointId" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/InstanceConnectEndpointId" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",

```

```

    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "InstanceConnectEndpointId"
        ]
      },
      "Null" : {
        "aws:RequestTag/InstanceConnectEndpointId" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/InstanceConnectEndpointId" : [
          "eice-*"
        ]
      }
    }
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2InstanceProfileForImageBuilder

EC2InstanceProfileForImageBuilder é uma [política AWS gerenciada](#) que: Perfil de instância EC2 para o serviço Image Builder.

## A utilização desta política

Você pode vincular a `EC2InstanceProfileForImageBuilder` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de dezembro de 2019, 19:08 UTC
- Horário editado: 27 de agosto de 2020, 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "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/*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EC2InstanceProfileForImageBuilderECRContainerBuilds

EC2InstanceProfileForImageBuilderECRContainerBuilds é uma [política AWS gerenciada](#) que: Perfil de instância do EC2 para criar imagens de contêiner com o EC2 Image Builder. Essa política concede ao usuário amplas permissões para carregar imagens ECR.

## A utilização desta política

Você pode vincular a `EC2InstanceProfileForImageBuilderECRContainerBuilds` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de dezembro de 2020, 19:48 UTC
- Horário editado: 11 de dezembro de 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ]
    }
  ]
}
```



```

    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "kms:Decrypt"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
        "aws:CalledVia" : [
          "imagebuilder.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : "arn:aws:s3:::ec2imagebuilder*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ECRReplicationServiceRolePolicy

ECRReplicationServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pela replicação ECR

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 04 de dezembro de 2020, 22:11 UTC
- Horário editado: 04 de dezembro de 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElastiCacheServiceRolePolicy

ElastiCacheServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa política ElastiCache permite gerenciar AWS recursos em seu nome conforme necessário para gerenciar seu cache

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de dezembro de 2017, 17:50 UTC
- Horário editado: 28 de novembro de 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
```

```
    "StringLike" : {
      "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
    }
  },
  {
    "Sid" : "TagVPCEndpointsOnCreation",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateVpcEndpoint",
        "aws:RequestTag/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/*"
  }
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElasticLoadBalancingFullAccess

ElasticLoadBalancingFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon ElasticLoadBalancing e acesso limitado a outros serviços necessários para fornecer os recursos do ElasticLoadBalancing.

### A utilização desta política

Você pode vincular a ElasticLoadBalancingFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 20 de setembro de 2018, 20:42 UTC
- Horário editado: 29 de novembro de 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

### Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "Action" : "elasticloadbalancing:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcClassicLink",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeClassicLinkInstances",
      "ec2:DescribeRouteTables",
      "ec2:DescribeCoipPools",
      "ec2:GetCoipPoolUsage",
      "ec2: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" : "*"
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElasticLoadBalancingReadOnly

ElasticLoadBalancingReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura à Amazon ElasticLoadBalancing e aos serviços dependentes

### Utilização desta política

Você pode vincular a ElasticLoadBalancingReadOnly aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 20 de setembro de 2018, 20:17 UTC
- Horário editado: 26 de novembro de 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalActivationsDownloadSoftwareAccess

ElementalActivationsDownloadSoftwareAccess é uma [política AWS gerenciada](#) que: Acesso para visualizar ativos adquiridos e baixar software relacionado e arquivos de inicialização

### A utilização desta política

Você pode vincular a ElementalActivationsDownloadSoftwareAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 08 de setembro de 2020, 17:26 UTC
- Horário editado: 08 de setembro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalActivationsFullAccess

ElementalActivationsFullAccess é uma [política AWS gerenciada](#) que: Acesso total para visualizar e agir sobre os ativos adquiridos da Elemental Appliances and Software

### A utilização desta política

Você pode vincular a ElementalActivationsFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 04 de junho de 2020, 21:00 UTC
- Horário editado: 04 de junho de 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalActivationsGenerateLicenses

ElementalActivationsGenerateLicenses é uma [política AWS gerenciada](#) que: Acesso para visualizar ativos adquiridos e gerar licenças de software para ativações pendentes

## A utilização desta política

Você pode vincular a `ElementalActivationsGenerateLicenses` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de agosto de 2020, 18:28 UTC
- Horário editado: 28 de agosto de 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalActivationsReadOnlyAccess

ElementalActivationsReadOnlyAccess é uma [política AWS gerenciada](#) que: Acesso somente para leitura à lista detalhada dos ativos adquiridos associados ao Conta da AWS do usuário

### A utilização desta política

Você pode vincular a ElementalActivationsReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 28 de agosto de 2020, 16:51 UTC
- Horário editado: 28 de agosto de 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalAppliancesSoftwareFullAccess

ElementalAppliancesSoftwareFullAccess é uma [política AWS gerenciada](#) que: Acesso total para visualizar e agir sobre cotações e pedidos de Elemental Appliances and Software

### A utilização desta política

Você pode vincular a ElementalAppliancesSoftwareFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 31 de julho de 2019, 16:28 UTC
- Horário editado: 05 de fevereiro de 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalAppliancesSoftwareReadOnlyAccess

ElementalAppliancesSoftwareReadOnlyAccess é uma [política AWS gerenciada](#) que: acesso somente de leitura para visualizar cotações e pedidos de equipamentos e software Elemental



## A utilização desta política

Você pode vincular a `ElementalAppliancesSoftwareReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 01 de abril de 2020, 22:31 UTC
- Horário editado: 01 de abril de 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ElementalSupportCenterFullAccess

ElementalSupportCenterFullAccess é uma [política AWS gerenciada](#) que: Acesso total para visualizar e agir sobre casos de suporte e conteúdo de suporte de produtos da Elemental Appliance and Software

### A utilização desta política

Você pode vincular a ElementalSupportCenterFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de novembro de 2020, 18:08 UTC
- Horário editado: 05 de fevereiro de 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "elemental-support-cases:*",
      "elemental-support-content:*",
      "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL é uma [política AWS gerenciada](#) que: Essa política concede permissões somente de leitura que permitem que o serviço WAL do Amazon EMR encontre e retorne o status de um cluster

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de junho de 2023, 23:30 UTC
- Horário editado: 15 de junho de 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## FMSServiceRolePolicy

FMSServiceRolePolicy é uma [política AWS gerenciada que: Política](#) de acesso para permitir que a função vinculada ao serviço de FM execute ações relacionadas à FM em recursos gerenciados por FM em uma conta da organização do cliente. AWS

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 28 de março de 2018, 23:01 UTC
- Horário editado: 21 de abril de 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

## Versão da política

Versão da política: v28 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:regional/webacl/*",
    "arn:aws:wafv2:*:*:global/webacl/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "waf:CreateWebACL",
    "waf-regional:CreateWebACL",
    "waf:GetChangeToken",
    "waf-regional:GetChangeToken",
    "waf-regional:GetWebACLForResource"
  ],
  "Resource" : [
    "arn:aws:waf:*:*:*",
    "arn:aws:waf-regional:*:*:*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
    "elasticloadbalancing:DescribeTags"
  ],

```

```

    "Resource" : "*"
  },
  {
    "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/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudfront:GetDistribution",
      "cloudfront:UpdateDistribution",
      "cloudfront>ListDistributionsByWebACLId",
      "cloudfront>ListDistributions"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "config>DeleteConfigRule",
      "config:GetComplianceDetailsByConfigRule",
      "config:PutConfigRule",
      "config:StartConfigRulesEvaluation"
    ],
    "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/"
  }
]

```

```

    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus",
    "config:PutConfigurationRecorder",
    "config:StartConfigurationRecorder",
    "config:PutDeliveryChannel",
    "config:DescribeDeliveryChannels",
    "config:DescribeDeliveryChannelStatus",
    "config:GetComplianceSummaryByConfigRule",
    "config:GetDiscoveredResourceCounts",
    "config:PutEvaluations",
    "config>SelectResourceConfig"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "config:DescribeConfigRuleEvaluationStatus",
    "config:DescribeConfigRules",
    "organizations:ListAccounts",
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListChildren",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{

```



```

    "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" : "*"
  },
  {
    "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/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeInstances"
    ]
  },

```

```
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2>DeleteTags",
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/FMManaged" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup",
      "ec2:DescribeSecurityGroupReferences",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeStaleSecurityGroups",
      "ec2:DescribeNetworkInterfaces",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcPeeringConnections"
    ],
    "Resource" : [
```

```

    "*"
  ]
},
{
  "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/*"
  ]
},
{
  "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/regexpruleset/*",
    "arn:aws:wafv2::*:regional/regexpruleset/*"
  ]
},
{
  "Effect" : "Allow",

```

```

    "Action" : [
      "wafv2:PutPermissionPolicy",
      "wafv2:GetPermissionPolicy",
      "wafv2>DeletePermissionPolicy"
    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:global/rulegroup/*",
      "arn:aws:wafv2:*:*:regional/rulegroup/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudfront:ListTagsForResource"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "wafv2:GetWebACLForResource"
    ],
    "Resource" : [
      "arn:aws:wafv2:*:*:regional/webacl/*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:route-table/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateRouteTable"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",

```

```
"Action" : "ec2:CreateTags",
"Resource" : [
  "arn:aws:ec2:*:*:subnet/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2>DeleteRouteTable",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
```

```

    "ec2:AssociateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateRouteTable",
    "ec2>DeleteSubnet",
    "ec2:DisassociateRouteTable",
    "ec2:ReplaceRouteTableAssociation"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInternetGateways",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/FMManaged" : [
        "true"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateVpcEndpoint",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{

```

```
"Effect" : "Allow",
"Action" : [
  "ec2:DeleteVpcEndpoints"
],
"Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
"Condition" : {
  "StringEquals" : {
    "ec2:ResourceTag/FMManaged" : "true"
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:TagResource"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:resource-share/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
}
},
{
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
}
},
{
  "Effect" : "Allow",
```

```
"Action" : "ram:CreateResourceShare",
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  },
  "StringEquals" : {
    "aws:RequestTag/FMManaged" : [
      "true"
    ]
  }
},
{
  "Sid" : "ram",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "network-firewall.amazonaws.com",
        "shield.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "*"
},
{
```



```

    "Effect" : "Allow",
    "Action" : [
      "network-firewall:TagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "Name",
          "FMManaged"
        ]
      }
    }
  },
  {
    "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" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "network-firewall>DeleteFirewallPolicy",

```

```
    "network-firewall:DeleteFirewall"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:ListLogDeliveries",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:ListFirewallRuleGroupAssociations",
    "route53resolver:ListTagsForResource",
    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroupAssociation",
    "route53resolver:GetFirewallRuleGroup",
    "route53resolver:GetFirewallRuleGroupPolicy",
    "route53resolver:PutFirewallRuleGroupPolicy"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:UpdateFirewallRuleGroupAssociation",
    "route53resolver:DisassociateFirewallRuleGroup"
  ],
  "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "route53resolver:AssociateFirewallRuleGroup",
      "route53resolver:TagResource"
    ],
    "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : "true"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess é uma [política AWS gerenciada](#) que: Permite que o Amazon FSx exclua suas funções vinculadas ao serviço para acesso ao Amazon S3

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Hora de criação: 28 de novembro de 2018, 10:40 UTC
- Horário editado: 28 de novembro de 2018, 10:40 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GameLiftGameServerGroupPolicy

GameLiftGameServerGroupPolicy é uma [política AWS gerenciada que: Política](#) para permitir que o Gamelift GameServerGroups gere os recursos do cliente

## A utilização desta política

Você pode vincular a `GameLiftGameServerGroupPolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 03 de abril de 2020, 23:12 UTC
- Horário editado: 13 de maio de 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:EnterStandby",
```

```

    "autoscaling:SetInstanceProtection",
    "autoscaling:UpdateAutoScalingGroup",
    "autoscaling:SuspendProcesses",
    "autoscaling:DetachInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/GameLift" : "GameServerGroups"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSubnets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "sns:Publish",
  "Resource" : [
    "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
    "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "AWS/GameLift"
    }
  }
}
]

```

```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GlobalAcceleratorFullAccess

GlobalAcceleratorFullAccess é uma [política AWS gerenciada](#) que: Permitir aos usuários do GlobalAccelerator acesso total a todas as APIs

### A utilização desta política

Você pode vincular a GlobalAcceleratorFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 02:44 UTC
- Horário editado: 04 de dezembro de 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```

"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "globalaccelerator:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeInstances",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeRegions",
      "ec2:DescribeSubnets"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
      }
    }
  }
]
}

```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)



- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GlobalAcceleratorReadOnlyAccess

GlobalAcceleratorReadOnlyAccess é uma [política AWS gerenciada](#) que: Permitir que usuários do GlobalAccelerator acessem APIs somente para leitura

### A utilização desta política

Você pode vincular a GlobalAcceleratorReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 02:41 UTC
- Horário editado: 27 de novembro de 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GreengrassOTAUpdateArtifactAccess

GreengrassOTAUpdateArtifactAccess é uma [política AWS gerenciada](#) que: Fornece acesso de leitura aos artefatos do Greengrass OTA Update em todas as regiões do Greengrass

### A utilização desta política

Você pode vincular a GreengrassOTAUpdateArtifactAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 29 de novembro de 2017, 18:11 UTC
- Horário editado: 18 de dezembro de 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GroundTruthSyntheticConsoleFullAccess

GroundTruthSyntheticConsoleFullAccess é uma [política AWS gerenciada](#) que: Essa política concede as permissões necessárias para usar todos os recursos do SageMaker Ground Truth Synthetic Console.

## A utilização desta política

Você pode vincular a `GroundTruthSyntheticConsoleFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de agosto de 2022, 15:58 UTC
- Horário editado: 25 de agosto de 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## GroundTruthSyntheticConsoleReadOnlyAccess

GroundTruthSyntheticConsoleReadOnlyAccess é uma [política gerenciada da AWS](#) que: Essa política concede acesso somente para leitura ao SageMaker Ground Truth Synthetic por meio do AWS Management Console.

### A utilização desta política

Você pode vincular a GroundTruthSyntheticConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 25 de agosto de 2022, 15:58 UTC
- Horário editado: 25 de agosto de 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "Effect" : "Allow",
    "Action" : [
      "sagemaker-groundtruth-synthetic:List*",
      "sagemaker-groundtruth-synthetic:Get*",
      "s3:ListBucket"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## Health\_OrganizationsServiceRolePolicy

Health\_OrganizationsServiceRolePolicy é uma [política gerenciada pela AWS](#): Política de saúde AWS para habilitar o recurso de exibição organizacional

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 16 de dezembro de 2019, 13:28 UTC
- Horário editado: 06 de fevereiro de 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMAccessAdvisorReadOnly

IAMAccessAdvisorReadOnly é uma [política AWS gerenciada](#) que: Essa política concede acesso para ler todas as informações de acesso fornecidas pelo consultor de acesso do IAM, como as informações do último acesso do serviço.

## A utilização desta política

Você pode vincular a `IAMAccessAdvisorReadOnly` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 21 de junho de 2019, 19:33 UTC
- Horário editado: 21 de junho de 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",

```



```
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribePolicy",
    "organizations:ListChildren",
    "organizations:ListParents",
    "organizations:ListPoliciesForTarget",
    "organizations:ListRoots",
    "organizations:ListPolicies",
    "organizations:ListTargetsForPolicy"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMAccessAnalyzerFullAccess

IAMAccessAnalyzerFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao IAM Access Analyzer

### A utilização desta política

Você pode vincular a IAMAccessAnalyzerFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 02 de dezembro de 2019, 17:12 UTC
- Horário editado: 02 de dezembro de 2019, 17:12 UTC

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

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
```

```
    "organizations:ListDelegatedAdministrators",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListParents",
    "organizations:ListRoots"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMAccessAnalyzerReadOnlyAccess

IAMAccessAnalyzerReadOnlyAccess é uma [política gerenciada pela AWS](#) que: fornece acesso somente leitura aos recursos do IAM Access Analyzer

### Utilização desta política

Você pode vincular a IAMAccessAnalyzerReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 02 de dezembro de 2019, 17:12 UTC
- Horário editado: 27 de novembro de 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMFullAccess

IAMFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao IAM por meio do AWS Management Console.

## A utilização desta política

Você pode vincular a `IAMFullAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 21 de junho de 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMReadOnlyAccess

IAMReadOnlyAccess é uma [política gerenciada da AWS](#) que: fornece acesso somente leitura ao IAM por meio de AWS Management Console.

### A utilização desta política

Você pode vincular a IAMReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:40 UTC
- Horário editado: 25 de janeiro de 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMSelfManageServiceSpecificCredentials

IAMSelfManageServiceSpecificCredentials é uma [política AWS gerenciada](#) que: permite que um usuário do IAM gere suas próprias credenciais específicas de serviço.

### A utilização desta política

Você pode vincular a IAMSelfManageServiceSpecificCredentials aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de dezembro de 2016, 17:25 UTC
- Horário editado: 22 de dezembro de 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam>DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)



- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMUserChangePassword

IAMUserChangePassword é uma [política AWS gerenciada](#) que: Fornece a capacidade de um usuário do IAM alterar sua própria senha.

### A utilização desta política

Você pode vincular a IAMUserChangePassword aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 15 de novembro de 2016, 00:25 UTC
- Horário editado: 15 de novembro de 2016, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    ],
    "Resource" : [
      "arn:aws:iam::*:user/${aws:username}"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:GetAccountPasswordPolicy"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IAMUserSSHKeys

IAMUserSSHKeys é uma [política AWS gerenciada](#) que: Fornece a capacidade de um usuário do IAM gerenciar suas próprias chaves SSH.

## A utilização desta política

Você pode vincular a IAMUserSSHKeys aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de julho de 2015, 17:08 UTC
- Horário editado: 09 de julho de 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# IVSFullAccess

IVSFullAccess é uma [política AWS gerenciada](#) que: fornece acesso total ao Interactive Video Service (IVS). Também inclui permissões para serviços dependentes, necessários para acesso total ao console ivs.

## Utilização desta política

Você pode vincular a IVSFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 13 de dezembro de 2023, 21:20 UTC
- Horário editado: 13 de dezembro de 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

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

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## IVSReadOnlyAccess

IVSReadOnlyAccess é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura às APIs de baixa latência e streaming em tempo real do IVS

### Utilização desta política

Você pode vincular a IVSReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 05 de dezembro de 2023, 18:00 UTC
- Horário editado: 16 de fevereiro de 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## IVSRecordToS3

IVSRecordToS3 é uma [política AWS gerenciada](#) que: Função vinculada ao serviço para realizar o S3 PutObject na gravação de transmissões ao vivo do IVS

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de dezembro de 2020, 00:10 UTC
- Horário editado: 05 de dezembro de 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::AWSIVS_*/ivs/*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa política concede permissão ao Kafka Connect para gerenciar AWS recursos em seu nome.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de setembro de 2021, 13:12 UTC
- Horário editado: 07 de setembro de 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`



## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
    }
  ]
}
```

```
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeNetworkInterfaces",
      "ec2:CreateNetworkInterfacePermission",
      "ec2:AttachNetworkInterface",
      "ec2:DetachNetworkInterface",
      "ec2>DeleteNetworkInterface"
    ],
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
      }
    }
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## KafkaServiceRolePolicy

KafkaServiceRolePolicy é uma [política AWS gerenciada que: política](#) de função vinculada ao serviço IAM para Kafka.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 15 de novembro de 2018, 23:31 UTC
- Horário editado: 28 de abril de 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
    }
  ]
}
```

```

    "Resource" : "arn:*:ec2:*:*:subnet/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints",
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:ResourceTag/AWSMSKManaged" : "true"
      },
      "StringLike" : {
        "ec2:ResourceTag/ClusterArn" : "*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetResourcePolicy",
      "secretsmanager:PutResourcePolicy",
      "secretsmanager>DeleteResourcePolicy",
      "secretsmanager:DescribeSecret"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
      }
    }
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy é uma [política AWS gerenciada](#) que: Permissões exigidas pela Keyspaces para replicação de dados entre regiões

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de maio de 2023, 16:15 UTC
- Horário editado: 02 de maio de 2023, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ]
    }
  ],
}
```

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## LakeFormationDataAccessServiceRolePolicy

LakeFormationDataAccessServiceRolePolicy é uma [política gerenciada pela AWS](#): Política para conceder acesso temporário aos dados dos recursos do Lake Formation

### Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

### Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 20 de junho de 2019, 20:46 UTC
- Horário editado: 06 de fevereiro de 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

### Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## LexBotPolicy

LexBotPolicy é uma [política AWS gerenciada que: Política](#) para o caso de uso do AWS Lex Bot

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de fevereiro de 2017, 22:18 UTC
- Horário editado: 13 de novembro de 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)



# LexChannelPolicy

LexChannelPolicy é uma [política AWS gerenciada que: Política](#) para o caso de uso do AWS Lex Channel

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 17 de fevereiro de 2017, 23:23 UTC
- Horário editado: 17 de fevereiro de 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

```
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## LightsailExportAccess

LightsailExportAccess é uma [política AWS gerenciada](#) que: política de função vinculada ao AWS Lightsail serviço que concede permissões para exportar recursos

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 28 de setembro de 2018, 16:35 UTC
- Horário editado: 15 de janeiro de 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:CopySnapshot",
      "ec2:DescribeSnapshots",
      "ec2:CopyImage",
      "ec2:DescribeImages"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetAccountPublicAccessBlock"
    ],
    "Resource" : "*"
  }
]
}

```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MediaConnectGatewayInstanceRolePolicy

MediaConnectGatewayInstanceRolePolicy é uma [política AWS gerenciada que: Essa política concede permissão para registrar instâncias do MediaConnect Gateway em um MediaConnect Gateway.](#)

## A utilização desta política

Você pode vincular a `MediaConnectGatewayInstanceRolePolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 22 de março de 2023, 20:43 UTC
- Horário editado: 22 de março de 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediacconnect:DiscoverGatewayPollEndpoint",
        "mediacconnect:PollGateway",
        "mediacconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MediaPackageServiceRolePolicy

MediaPackageServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o MediaPackage publique registros no CloudWatch

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de setembro de 2020, 17:45 UTC
- Horário editado: 18 de setembro de 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "logs:PutLogEvents",
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MemoryDBServiceRolePolicy

MemoryDBServiceRolePolicy é uma [política AWS gerenciada](#) que: Esta política permite que o MemoryDB gerencie AWS recursos em seu nome, conforme necessário para gerenciar seus recursos.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 17 de agosto de 2021, 22:34 UTC
- Horário editado: 18 de agosto de 2021, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MigrationHubDMSAccessServiceRolePolicy

MigrationHubDMSAccessServiceRolePolicy é uma [política AWS gerenciada que: Política](#) para que o Database Migration Service assuma uma função na conta do cliente para ligar para o Migration Hub

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de junho de 2019, 17:50 UTC
- Horário editado: 07 de outubro de 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MigrationHubServiceRolePolicy

MigrationHubServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que o Migration Hub chame o Application Discovery Service em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de junho de 2019, 17:22 UTC
- Horário editado: 06 de agosto de 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Effect" : "Allow",
"Action" : [
  "discovery:ListConfigurations",
  "discovery:DescribeConfigurations"
],
"Resource" : [
  "*"
]
},
{
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "aws:migrationhub:source-id"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "dms:AddTagsToResource",
  "Resource" : [
    "arn:aws:dms:*:*:endpoint:*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "aws:migrationhub:source-id"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstanceAttribute"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MigrationHubSMSAccessServiceRolePolicy

MigrationHubSMSAccessServiceRolePolicy é uma [política AWS gerenciada que: Política](#) para que o Serviço de Migração de Servidores assuma uma função na conta do cliente para ligar para o Migration Hub

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de junho de 2019, 18:30 UTC
- Horário editado: 07 de outubro de 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)

- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## MonitronServiceRolePolicy

MonitronServiceRolePolicy é uma [política AWS gerenciada que: Política](#) para a função vinculada ao serviço da AWS Monitron que concede acesso aos recursos necessários do cliente.

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 02 de maio de 2022, 19:22 UTC
- Horário editado: 02 de maio de 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## NeptuneConsoleFullAccess

NeptuneConsoleFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total para gerenciar o Amazon Neptune usando o AWS Management Console. Observe que essa política também concede acesso total para publicar em todos os tópicos do SNS dentro da conta, permissões para criar e editar instâncias do Amazon EC2 e configurações de VPC, permissões para visualizar e listar chaves no Amazon KMS e acesso total ao Amazon RDS. Para obter mais informações, consulte <https://aws.amazon.com/neptune/faqs/>.

## Utilização desta política

Você pode vincular a NeptuneConsoleFullAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 19 de junho de 2018, 21:35 UTC
- Horário editado: 30 de novembro de 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

## Versão da política

Versão da política: v5 (padrão)



A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds>CreateDBClusterParameterGroup",
        "rds>CreateDBClusterSnapshot",
        "rds>CreateDBParameterGroup",
        "rds>CreateDBSubnetGroup",
        "rds>CreateEventSubscription",
```

```
"rds:DeleteDBCluster",
"rds:DeleteDBClusterParameterGroup",
"rds:DeleteDBClusterSnapshot",
"rds:DeleteDBInstance",
"rds:DeleteDBParameterGroup",
"rds:DeleteDBSubnetGroup",
"rds:DeleteEventSubscription",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
```

```
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "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"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## NeptuneFullAccess

NeptuneFullAccess é uma [política gerenciada pela AWS](#) que: fornece acesso total ao Amazon Neptune. Observe que essa política também concede acesso total para publicar em todos os tópicos do SNS dentro da conta e acesso total ao Amazon RDS. Para obter mais informações, consulte <https://aws.amazon.com/neptune/faqs/>.

## Utilização desta política

Você pode vincular a `NeptuneFullAccess` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 30 de maio de 2018, 19:17 UTC
- Horário editado: 22 de janeiro de 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "AllowManagementPermissionsForRDS",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddRoleToDBCluster",
    "rds:AddSourceIdentifierToSubscription",
    "rds:AddTagsToResource",
    "rds:ApplyPendingMaintenanceAction",
    "rds:CopyDBClusterParameterGroup",
    "rds:CopyDBClusterSnapshot",
    "rds:CopyDBParameterGroup",
    "rds>CreateDBClusterEndpoint",
    "rds>CreateDBClusterParameterGroup",
    "rds>CreateDBClusterSnapshot",
    "rds>CreateDBParameterGroup",
    "rds>CreateDBSubnetGroup",
    "rds>CreateEventSubscription",
    "rds>CreateGlobalCluster",
    "rds>DeleteDBCluster",
    "rds>DeleteDBClusterEndpoint",
    "rds>DeleteDBClusterParameterGroup",
    "rds>DeleteDBClusterSnapshot",
    "rds>DeleteDBInstance",
    "rds>DeleteDBParameterGroup",
    "rds>DeleteDBSubnetGroup",
    "rds>DeleteEventSubscription",
    "rds>DeleteGlobalCluster",
    "rds:DescribeDBClusterEndpoints",
    "rds:DescribeAccountAttributes",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBClusterSnapshotAttributes",
    "rds:DescribeDBClusterSnapshots",
    "rds:DescribeDBClusters",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBLogFiles",
    "rds:DescribeDBParameterGroups",
    "rds:DescribeDBParameters",
    "rds:DescribeDBSecurityGroups",
```



```

    "rds:DescribeDBSubnetGroups",
    "rds:DescribeEngineDefaultClusterParameters",
    "rds:DescribeEngineDefaultParameters",
    "rds:DescribeEventCategories",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeEvents",
    "rds:DescribeGlobalClusters",
    "rds:DescribeOptionGroups",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DescribeValidDBInstanceModifications",
    "rds:DownloadDBLogFilePortion",
    "rds:FailoverDBCluster",
    "rds:FailoverGlobalCluster",
    "rds:ListTagsForResource",
    "rds:ModifyDBCluster",
    "rds:ModifyDBClusterEndpoint",
    "rds:ModifyDBClusterParameterGroup",
    "rds:ModifyDBClusterSnapshotAttribute",
    "rds:ModifyDBInstance",
    "rds:ModifyDBParameterGroup",
    "rds:ModifyDBSubnetGroup",
    "rds:ModifyEventSubscription",
    "rds:ModifyGlobalCluster",
    "rds:PromoteReadReplicaDBCluster",
    "rds:RebootDBInstance",
    "rds:RemoveFromGlobalCluster",
    "rds:RemoveRoleFromDBCluster",
    "rds:RemoveSourceIdentifierFromSubscription",
    "rds:RemoveTagsFromResource",
    "rds:ResetDBClusterParameterGroup",
    "rds:ResetDBParameterGroup",
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime",
    "rds:StartDBCluster",
    "rds:StopDBCluster"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "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" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## NeptuneGraphReadOnlyAccess

NeptuneGraphReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura a todos os recursos do Amazon Neptune Analytics, além de permissões somente de leitura para serviços dependentes.

### Utilização desta política

Você pode vincular a NeptuneGraphReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 30 de novembro de 2023, 07:32 UTC

- Horário editado: 30 de novembro de 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
```

```
    "Effect" : "Allow",
    "Action" : [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics",
      "cloudwatch:GetMetricStatistics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# NeptuneReadOnlyAccess

NeptuneReadOnlyAccess é uma [política gerenciada pela AWS](#) que: fornece acesso somente de leitura ao Amazon Neptune. Observe que essa política também concede acesso a recursos do Amazon RDS. Para obter mais informações, consulte <https://aws.amazon.com/neptune/faqs/>.

## Utilização desta política

Você pode vincular a NeptuneReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 30 de maio de 2018, 19:16 UTC
- Horário editado: 22 de janeiro de 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
```

```
    "rds:DescribeDBClusters",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBLogFiles",
    "rds:DescribeDBParameterGroups",
    "rds:DescribeDBParameters",
    "rds:DescribeDBSubnetGroups",
    "rds:DescribeEventCategories",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeEvents",
    "rds:DescribeGlobalClusters",
    "rds:DescribeOrderableDBInstanceOptions",
    "rds:DescribePendingMaintenanceActions",
    "rds:DownloadDBLogFilePortion",
    "rds:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadOnlyPermissionsForKMS",
  "Effect" : "Allow",
```

```
    "Action" : [
      "kms:ListKeys",
      "kms:ListRetirableGrants",
      "kms:ListAliases",
      "kms:ListKeyPolicies"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
      "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
    ]
  },
  {
    "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
    "Effect" : "Allow",
    "Action" : [
      "neptune-db:Read*",
      "neptune-db:Get*",
      "neptune-db:List*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)



- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## NetworkAdministrator

NetworkAdministrator é uma [política AWS gerenciada](#) que: Concede permissões de acesso total aos AWS serviços e ações necessários para instalar e configurar recursos AWS de rede.

### A utilização desta política

Você pode vincular a NetworkAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:31 UTC
- Horário editado: 16 de setembro de 2021, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

### Versão da política

Versão da política: v11 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## OAMFullAccess

OAMFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao CloudWatch Observability Access Manager

## A utilização desta política

Você pode vincular a OAMFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2022, 13:38 UTC
- Horário editado: 27 de novembro de 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

## Versão da política

Versão da política: v1 (padrão)



A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## OAMReadOnlyAccess

OAMReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao CloudWatch Observability Access Manager

## A utilização desta política

Você pode vincular a OAMReadOnlyAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 27 de novembro de 2022, 13:29 UTC
- Horário editado: 27 de novembro de 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# PartnerCentralAccountManagementUserRoleAssociation

PartnerCentralAccountManagementUserRoleAssociation é uma [política gerenciada pela AWS](#) que: fornece acesso para associar e dissociar usuários centrais de parceiros com funções do IAM

## Utilização desta política

Você pode vincular a PartnerCentralAccountManagementUserRoleAssociation aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 10 de novembro de 2023, 02:03 UTC
- Hora da edição: 10 de novembro de 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
    }
  ]
}
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## PowerUserAccess

PowerUserAccess é uma [política AWS gerenciada](#) que: fornece acesso total aos AWS serviços e recursos, mas não permite o gerenciamento de usuários e grupos.

### A utilização desta política

Você pode vincular a PowerUserAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS

- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 06 de julho de 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## QuickSightAccessForS3StorageManagementAnalyticsReadOnly

QuickSightAccessForS3StorageManagementAnalyticsReadOnly é uma [política AWS gerenciada](#) que: Política usada pela equipe do QuickSight para acessar dados de clientes produzidos pelo S3 Storage Management Analytics.

### A utilização desta política

Você pode vincular a QuickSightAccessForS3StorageManagementAnalyticsReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 12 de junho de 2017, 18:18 UTC
- Horário editado: 08 de outubro de 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

### Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## RDSCloudHsmAuthorizationRole

RDSCloudHsmAuthorizationRole é uma [política AWS gerenciada](#) que: Política padrão para a função de serviço do Amazon RDS.

## A utilização desta política

Você pode vincular a `RDSCloudHsmAuthorizationRole` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 26 de setembro de 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```



## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ReadOnlyAccess

ReadOnlyAccess é uma [política AWS gerenciada](#) que: fornece acesso somente de leitura aos AWS serviços e recursos.

### Utilização desta política

Você pode vincular a ReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 05 de fevereiro de 2024, 15:00 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

### Versão da política

Versão da política: v111 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

### Documento da política JSON

```
{
  "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:BatchGetVpcEndpoint",
"aoss:GetAccessPolicy",
"aoss:GetAccountSettings",
"aoss:GetPoliciesStats",
"aoss:GetSecurityConfig",
"aoss:GetSecurityPolicy",
"aoss:ListAccessPolicies",
"aoss:ListCollections",
"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:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appstream:Describe*",
"appstream:List*",
"appsync:Get*",
"appsync:List*",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"aps:DescribeRuleGroupsNamespace",
"aps:DescribeWorkspace",
"aps:GetAlertManagerSilence",
"aps:GetAlertManagerStatus",
"aps:GetLabels",
"aps:GetMetricMetadata",
"aps:GetSeries",
"aps:ListAlertManagerAlertGroups",
"aps:ListAlertManagerAlerts",
"aps:ListAlertManagerReceivers",
"aps:ListAlertManagerSilences",
```

```
"aps:ListAlerts",
"aps:ListRuleGroupsNamespaces",
"aps:ListRules",
"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: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: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: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",
"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:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListMembers",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"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:GetLogLevelByResourceTypes",
"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:GetPlaybackKeyPair",
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListPlaybackKeyPairs",
"ivs:ListRecordingConfigurations",
"ivs:ListStreams",
"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:ListChannels",
"medialive:ListInputDevices",
"medialive:ListInputDeviceTransfers",
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"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",
"qldb:ListTagsForResource",
"ram:Get*",
"ram:List*",
"rbin:GetRule",
"rbin:ListRules",
"rbin:ListTagsForResource",
"rds:Describe*",
"rds:Download*",
"rds:List*",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"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",
```

```
"resiliencyhub: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*",
"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*",
"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",
"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*",
"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" : "*"

```

```
}  
  ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## ResourceGroupsandTagEditorFullAccess

ResourceGroupsandTagEditorFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Resource Groups and Tag Editor.

### A utilização desta política

Você pode vincular a ResourceGroupsandTagEditorFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 10 de agosto de 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ResourceGroupsandTagEditorReadOnlyAccess

ResourceGroupsandTagEditorReadOnlyAccess é uma [política AWS gerenciada](#) que: fornece acesso ao uso do Resource Groups e do Tag Editor, mas não permite a edição de tags por meio do Tag Editor.

## A utilização desta política

Você pode vincular a `ResourceGroupsandTagEditorReadOnlyAccess` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:39 UTC
- Horário editado: 10 de agosto de 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

## Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ResourceGroupsServiceRolePolicy

ResourceGroupsServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que AWS Resource Groups consultem os AWS serviços que possuem seus recursos para manter o grupo atualizado

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 05 de janeiro de 2023, 16:57 UTC
- Horário editado: 05 de janeiro de 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy é uma [política AWS gerenciada](#) que: permite que o operador do driver OpenShift Amazon EBS Container Storage Interface (CSI) instale e mantenha o driver CSI do Amazon EBS em um cluster Red Hat OpenShift Service on (ROSA). AWS O driver da CSI do Amazon EBS permite que os clusters do ROSA gerenciem o ciclo de vida dos volumes do Amazon EBS para os volumes persistentes.

### A utilização desta política

Você pode vincular a ROSAAmazonEBSCSIDriverOperatorPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço

- Horário de criação: 20 de abril de 2023, 22:36 UTC
- Horário editado: 20 de abril de 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
        "aws:ResourceTag/red-hat-managed" : "true"
    }
}
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/red-hat-managed" : "true"
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVolume"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/red-hat-managed" : "true"
        }
    }
},
{
    "Sid" : "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"
        ]
    }
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy é uma [política AWS gerenciada](#) que: Permite que o Operador do OpenShift Cloud Network Config Controller provisione e gereencie recursos de rede para uso pelo Red Hat OpenShift Service AWS on (ROSA) cluster network overlay. O OpenShift Cloud Network Operator interage com as AWS APIs em nome dos plug-ins de rede por meio de CustomResourceDefinitions. O operador usa essas permissões de política para gerenciar endereços IP privados para instâncias do Amazon EC2 como parte do cluster ROSA.

## A utilização desta política

Você pode vincular a ROSACloudNetworkConfigOperatorPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de abril de 2023, 22:34 UTC
- Horário editado: 20 de abril de 2023, 22:34 UTC



- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAControlPlaneOperatorPolicy

ROSAControlPlaneOperatorPolicy é uma [política AWS gerenciada](#) que: Permite que o Red Hat OpenShift Service on AWS (ROSA) gerencie os recursos do cluster ROSA do Amazon EC2 e do Amazon Route 53.

### A utilização desta política

Você pode vincular a ROSAControlPlaneOperatorPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 24 de abril de 2023, 23:02 UTC
- Horário editado: 30 de junho de 2023, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "SecurityGroupIngressEgress",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroupsVPCNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*/*"
  ]
},
{
  "Sid" : "ListResourceRecordSets",
  "Effect" : "Allow",
  "Action" : [
    "route53:ListResourceRecordSets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
  "Effect" : "Allow",
```

```
"Action" : [
  "route53:ChangeResourceRecordSets"
],
"Resource" : [
  "*"
],
"Condition" : {
  "ForAllValues:StringLike" : {
    "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
      "*.hypershift.local"
    ]
  }
}
},
{
  "Sid" : "VPCEndpointWithCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "VPCEndpointResourceTagCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
}
},
```

```
{
  "Sid" : "VPCendpointNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:route-table/*"
  ]
},
{
  "Sid" : "ManageVPCendpointWithCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "ModifyVPCendpoingNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyVpcEndpoint"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
}
```

```
"Resource" : [
  "arn:aws:ec2:*:*:vpc-endpoint/*",
  "arn:aws:ec2:*:*:security-group/*"
],
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : [
      "CreateVpcEndpoint",
      "CreateSecurityGroup"
    ]
  }
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAImageRegistryOperatorPolicy

ROSAImageRegistryOperatorPolicy é uma [política AWS gerenciada](#) que: permite que o operador de registro de OpenShift imagens provisione e gerencie buckets e objetos do Amazon S3 para uso pelo Red Hat OpenShift Service on AWS (ROSA) no registro de imagens no cluster para atender aos requisitos de armazenamento do ROSA. O Operador de Registro de OpenShift Imagem instala e mantém o registro interno de um OpenShift cluster Red Hat.

## Utilização desta política

Você pode vincular a ROSAImageRegistryOperatorPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço

- Horário de criação: 27 de abril de 2023, 20:13 UTC
- Horário editado: 12 de dezembro de 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3>DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : [
      "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
      "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
    ]
  },
  {
    "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}/*"
    ]
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAIngressOperatorPolicy

ROSAIngressOperatorPolicy é uma [política AWS gerenciada](#) que: Permite que o OpenShift Ingress Operator provisione e gerencie balanceadores de carga e configurações de sistema de nomes de domínio (DNS) para clusters Red Hat OpenShift Service on (ROSA). AWS A política

permite acesso de leitura aos valores das tags, que o operador filtra para os recursos do Route 53 para descobrir zonas hospedadas.

## A utilização desta política

Você pode vincular a `ROSAIngressOperatorPolicy` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de abril de 2023, 22:37 UTC
- Horário editado: 20 de abril de 2023, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
          "*.openshiftapps.com",
          "*.devshift.org",
          "*.openshiftusgov.com",
          "*.devshiftusgov.com"
        ]
      }
    }
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAInstallerPolicy

ROSAInstallerPolicy é uma [política AWS gerenciada](#) que: Permite que o instalador do Red Hat OpenShift Service on AWS (ROSA) gerencie AWS recursos que suportam a instalação do cluster ROSA. Isso inclui o gerenciamento de perfis de instância para nós de trabalho ROSA.

## Utilização desta política

Você pode vincular a ROSAInstallerPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 06 de junho de 2023, 21:00 UTC
- Horário editado: 26 de janeiro de 2024, 21:04 UTC

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

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ]
    }
  ]
}
```

```

    ],
    "Resource" : "*"
  },
  {
    "Sid" : "PassRoleToEC2",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:*:iam:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  }
},
{
  "Sid" : "ManageInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ]
},
{
  "Sid" : "CreateInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateInstanceProfile",
    "iam:TagInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ],
  "Condition" : {

```

```
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  },
  {
    "Sid" : "GetSecretValue",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "Route53ManageRecords",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeResourceRecordSets"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
          "*.openshiftapps.com",
          "*.devshift.org",
          "*.hypershift.local",
          "*.openshiftusgov.com",
          "*.devshiftusgov.com"
        ]
      }
    }
  },
  {
    "Sid" : "Route53Manage",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeTagsForResource",
```

```

    "route53:CreateHostedZone",
    "route53>DeleteHostedZone"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "RunInstances"
      ]
    }
  }
},
{
  "Sid" : "RunInstancesNoCondition",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:snapshot*"
  ]
},
{
  "Sid" : "RunInstancesRestrictedRequestTag",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
        "aws:RequestTag/red-hat-managed" : "true"
    }
}
},
{
  "Sid" : "RunInstancesRedHatOwnedAMIs",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:Owner" : [
        "531415883065",
        "251351625822",
        "210686502322"
      ]
    }
  }
},
{
  "Sid" : "ManageInstancesRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances",
    "ec2:GetConsoleOutput"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateGrantRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
```



```
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat" : "true"
  },
  "StringLike" : {
    "kms:ViaService" : "ec2.*.amazonaws.com"
  },
  "Bool" : {
    "kms:GrantIsForAWSResource" : true
  }
},
{
  "Sid" : "ManagedKMSRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DeleteSecurityGroup",
  "Effect" : "Allow",
```

```
"Action" : [
  "ec2:DeleteSecurityGroup"
],
"Resource" : [
  "arn:aws:ec2:*:*:security-group/*/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat-managed" : "true"
  }
}
},
{
  "Sid" : "SecurityGroupIngressEgress",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroupsVPCNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
```

```
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup"
      ]
    }
  }
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAKMSProviderPolicy

ROSAKMSProviderPolicy é uma [política AWS gerenciada](#) que: permite que o provedor de AWS criptografia ROSA integrado gerencie as chaves do Serviço de Gerenciamento de Chaves (KMS) para oferecer suporte à criptografia de dados etcd usando uma AWS chave AWS KMS fornecida pelo cliente. A política permite a criptografia e a descriptografia de dados usando chaves KMS.

## A utilização desta política

Você pode vincular a ROSAKMSProviderPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço

- Horário de criação: 27 de abril de 2023, 20:10 UTC
- Horário editado: 27 de abril de 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAKubeControllerPolicy

ROSAKubeControllerPolicy é uma [política AWS gerenciada](#) que: permite que o controlador ROSA Kubernetes gerencie os recursos do Amazon EC2, do Elastic Load Balancing (ELB) e do AWS Key Management Service (KMS) para um cluster ROSA.

### A utilização desta política

Você pode vincular a ROSAKubeControllerPolicy aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 27 de abril de 2023, 20:09 UTC
- Horário editado: 16 de outubro de 2023, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

### Versão da política

Versão da política: v3 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeInstances",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticloadbalancing:DescribeLoadBalancerPolicies"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "KMSDescribeKey",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "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"
    }
  }
}
```

```
}  
 ]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAManageSubscription

ROSAManageSubscription é uma [política AWS gerenciada](#) que: Essa política fornece as permissões necessárias para gerenciar a assinatura do Red Hat OpenShift Service on AWS (ROSA).

### A utilização desta política

Você pode vincular a ROSAManageSubscription aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 11 de abril de 2022, 20:58 UTC
- Horário editado: 04 de agosto de 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# ROSANodePoolManagementPolicy

ROSANodePoolManagementPolicy é uma [política AWS gerenciada](#) que: Permite que o Red Hat OpenShift Service on AWS (ROSA) gerencie instâncias EC2 de cluster como nós de trabalho, incluindo permissão para configurar grupos de segurança e marcar instâncias e volumes. Essa política também permite o uso de instâncias do EC2 com criptografia de disco fornecida pelas AWS chaves do Key Management Service (KMS).

## A utilização desta política

Você pode vincular a ROSANodePoolManagementPolicy aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 08 de junho de 2023, 20:48 UTC
- Horário editado: 08 de junho de 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSASRESupportPolicy

ROSASRESupportPolicy é uma [política AWS gerenciada](#) que: fornece à engenharia de confiabilidade do site (SRE) do ROSA as permissões necessárias para observar, diagnosticar e oferecer suporte inicialmente aos AWS recursos associados ao Red Hat OpenShift Service on AWS (ROSA) clusters, incluindo a capacidade de alterar o estado do nó do cluster ROSA.

## Utilização desta política

Você pode vincular a ROSASRESupportPolicy aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: Política de função de serviço
- Horário de criação: 01 de junho de 2023, 14:36 UTC
- Horário editado: 22 de janeiro de 2024, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou perfil com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se concederá a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "EC2DescribeInstance",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "VPCNetwork",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "Cloudtrail",
    "Effect" : "Allow",
    "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
    ],
    "Resource" : [
        "*"
    ]
},
{
```

```
"Sid" : "Cloudwatch",
"Effect" : "Allow",
"Action" : [
  "cloudwatch:GetMetricData",
  "cloudwatch:GetMetricStatistics",
  "cloudwatch:ListMetrics"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "DescribeVolumes",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumesModifications",
    "ec2:DescribeVolumeStatus"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeLoadBalancers",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeAccountLimits",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeListenerCertificates",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeSSLPolicies",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : [
    "*"
  ]
}
```

```
]
},
{
  "Sid" : "DescribeVPC",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpointConnections",
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeStaleSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeAddressesAttribute",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeAddressesAttribute",
  "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
},
{
  "Sid" : "DescribeInstance",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "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"
    }
}
]
}
```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ROSAWorkerInstancePolicy

`ROSAWorkerInstancePolicy` é uma [política AWS gerenciada](#) que: Permite que o Red Hat OpenShift Service nos nós de trabalho AWS (ROSA) da sua conta tenha acesso somente de leitura às instâncias do Amazon EC2 e Regiões da AWS ao gerenciamento do ciclo de vida dos nós computacionais.

### A utilização desta política

Você pode vincular a `ROSAWorkerInstancePolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de abril de 2023, 22:35 UTC
- Horário editado: 20 de abril de 2023, 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.



## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## Route53RecoveryReadinessServiceRolePolicy

Route53RecoveryReadinessServiceRolePolicy é uma [política AWS gerenciada](#) que: Service Linked Role Policy for Route 53 Recovery Readiness

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço

- Horário de criação: 15 de julho de 2021, 16:06 UTC
- Horário editado: 14 de fevereiro de 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/AWSServiceRoleForServiceQuotas",
    }
  ]
}
```

```
"Condition" : {
  "StringLike" : {
    "iam:AWSServiceName" : "servicequotas.amazonaws.com"
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "lambda:GetFunctionConcurrency",
    "lambda:GetFunctionConfiguration",
    "lambda:GetProvisionedConcurrencyConfig",
    "lambda:ListProvisionedConcurrencyConfigs",
    "lambda:ListAliases",
    "lambda:ListVersionsByFunction"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBClusters"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBInstances"
  ],
  "Resource" : "arn:aws:rds:*:*:db:*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53:ListResourceRecordSets"
  ],
  "Resource" : "arn:aws:route53:::hostedzone/*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "route53:GetHealthCheck",
    "route53:GetHealthCheckStatus"
  ]
}
```

```
    ],
    "Resource" : "arn:aws:route53:::healthcheck/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:RequestServiceQuotaIncrease"
    ],
    "Resource" : "arn:aws:servicequotas:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sns:GetTopicAttributes",
      "sns:ListSubscriptionsByTopic"
    ],
    "Resource" : "arn:aws:sns:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sqs:GetQueueAttributes",
      "sqs:GetQueueUrl"
    ],
    "Resource" : "arn:aws:sqs:*:*:*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingPolicies",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeAutoScalingInstances",
      "autoscaling:DescribeLifecycleHooks",
      "autoscaling:DescribeLoadBalancers",
      "autoscaling:DescribeLoadBalancerTargetGroups",
      "autoscaling:DescribeNotificationConfigurations",
      "autoscaling:DescribePolicies",
      "cloudwatch:GetMetricData",
      "cloudwatch:DescribeAlarms",
      "dynamodb:DescribeLimits",
      "dynamodb:ListGlobalTables",
```

```
"dynamodb:ListTables",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeCustomerGateways",
"ec2:DescribeInstances",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetEbsDefaultKmsKeyId",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"kafka:DescribeCluster",
"kafka:DescribeConfigurationRevision",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"rds:DescribeAccountAttributes",
"route53:GetHostedZone",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"sns:GetEndpointAttributes",
"sns:GetSubscriptionAttributes"
],
"Resource" : "*"
}
]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# Route53ResolverServiceRolePolicy

Route53ResolverServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Route53 Resolver

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

## Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 12 de agosto de 2020, 17:47 UTC
- Horário editado: 12 de agosto de 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
```

```
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## S3StorageLensServiceRolePolicy

S3StorageLensServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo S3 Storage Lens

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 18 de novembro de 2020, 18:15 UTC
- Horário editado: 18 de novembro de 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## SecretsManagerReadWrite

SecretsManagerReadWrite é uma [política AWS gerenciada](#) que: Fornece acesso de leitura/gravação ao AWS Secrets Manager por meio do. AWS Management Console Observação: isso exclui ações do IAM, portanto, combine com o IAM FullAccess se a configuração de rotação for necessária.



## Utilização desta política

Você pode vincular a `SecretsManagerReadWrite` aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política AWS gerenciada
- Horário de criação: 04 de abril de 2018, 18:05 UTC
- Horário editado: 22 de fevereiro de 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

## Versão da política

Versão da política: v5 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
```

```

    "kms:ListAliases",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstances",
    "redshift:DescribeClusters",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "LambdaPermissions",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission",
    "lambda:CreateFunction",
    "lambda:GetFunction",
    "lambda:InvokeFunction",
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
},
{
  "Sid" : "SARPermissions",
  "Effect" : "Allow",
  "Action" : [
    "serverlessrepo:CreateCloudFormationChangeSet",
    "serverlessrepo:GetApplication"
  ],
  "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
},
{
  "Sid" : "S3Permissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::awsserverlessrepo-changesets*",
    "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
  ]
}

```

```
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas AWS gerenciadas no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## SecurityAudit

SecurityAudit é uma [política gerenciada pela AWS](#): O modelo de auditoria de segurança concede acesso para ler metadados de configuração de segurança. É útil para software que audita a configuração de uma Conta da AWS.

## Utilização desta política

Você pode vincular a SecurityAudit aos seus usuários, grupos e perfis.

## Detalhes desta política

- Tipo: política gerenciada pela AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 14 de dezembro de 2023, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

## Versão da política

Versão da política: v41 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função com esta política faz uma solicitação para acessar um atributo da AWS, a AWS verifica a versão padrão da política para determinar se irá conceder a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "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:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
```

```
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appsync:GetApiCache",
"appsync:List*",
"athena:GetWorkGroup",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentFrameworkShareRequests",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListControls",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling:Describe*",
"backup:DescribeRegionSettings",
"backup:GetBackupVaultAccessPolicy",
"backup:ListBackupVaults",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobDefinitions",
"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:GetTrail",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GetDashboard",
"cloudwatch:ListTagsForResource",
"cloudwatch:ListDashboards",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListRepositories",
"codebuild:BatchGetProjects",
"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:ListInstances",
"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:DescribeGlobalTable",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetImageBlockPublicAccessState",
"ec2:GetManagedPrefixListAssociations",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImages",
"ecr:DescribeImageScanFindings",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRegistryScanningConfiguration",
"ecr:GetRepositoryPolicy",
"ecr:ListImages",
```



```
"ecr:ListTagsForResource",
"ecs:Describe*",
"ecs:List*",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodeGroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodeGroups",
"eks:ListUpdates",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elastictranscoder:ListPipelines",
"es:Describe*",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListElasticsearchInstanceTypeDetails",
"es:ListElasticsearchVersions",
"es:ListTags",
"events:Describe*",
"events:List*",
"events:TestEventPattern",
"finespace:ListEnvironments",
"finespace: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:GetVaultAccessPolicy",
"glacier:GetVaultLock",
"glacier:ListVaults",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:GetCrawlers",
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfigurations",
"grafana:ListWorkspaces",
"greengrass:List*",
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
"health:DescribeAffectedEntities",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
"health:DescribeEvents",
"health:DescribeEventTypes",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
```

```
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"iot:Describe*",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:List*",
"iotanalytics:ListChannels",
"iotevents:ListInputs",
"iotfleetwise:ListModelManifests",
"iotsitewise:DescribeGatewayCapabilityConfiguration",
"iotsitewise:ListAssetModels",
"iotsitewise:ListGateways",
"iottwinmaker:ListWorkspaces",
"kafka-cluster:Describe*",
"kafka:Describe*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafkaconnect:Describe*",
"kafkaconnect:List*",
"kendra:DescribeIndex",
"kendra:ListIndices",
"kinesis:DescribeLimits",
"kinesis:DescribeStream",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListShards",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
```

```
"kinesisanalytics:ListApplications",
"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:GetDisks",
"lightsail:GetDiskSnapshots",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"machinelearning:DescribeMLModels",
"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",
"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: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:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemas",
"schemas:ListSchemaVersions",
```

```
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecrets",
"secretsmanager:ListSecretVersionIds",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"servicequotas:ListTagsForResource",
"ses:Describe*",
"ses:GetAccountSendingEnabled",
"ses:GetIdentityDkimAttributes",
"ses:GetIdentityPolicies",
"ses:GetIdentityVerificationAttributes",
"ses:ListConfigurationSets",
"ses:ListIdentities",
"ses:ListIdentityPolicies",
"ses:ListReceiptRuleSets",
"ses:ListVerifiedEmailAddresses",
"shield:Describe*",
"shield:GetSubscriptionState",
"shield:List*",
"snowball:ListClusters",
"snowball:ListJobs",
"sns:GetPlatformApplicationAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
```

```
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListQueues",
"sqs:ListQueueTags",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:ListAssociations",
"ssm:ListAssociationVersions",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocuments",
"ssm:ListDocumentVersions",
"ssm:ListInventoryEntries",
"ssm:ListOpsMetadata",
"ssm:ListResourceComplianceSummaries",
"ssm:ListResourceDataSync",
"ssm:ListTagsForResource",
"sso:DescribeAccountAssignmentCreationStatus",
"sso:DescribePermissionSet",
"sso:DescribePermissionsPolicies",
"sso: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:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics>ListAssociatedGroups",
"synthetics>ListGroupResources",
"synthetics>ListGroups",
"synthetics>ListTagsForResource",
"tag:GetResources",
"tag:GetTagKeys",
"transcribe:GetCallAnalyticsCategory",
"transcribe:GetMedicalVocabulary",
"transcribe:GetVocabulary",
"transcribe:GetVocabularyFilter",
"transcribe>ListCallAnalyticsCategories",
"transcribe>ListCallAnalyticsJobs",
"transcribe>ListLanguageModels",
"transcribe>ListMedicalTranscriptionJobs",
"transcribe>ListMedicalVocabularies",
"transcribe>ListTagsForResource",
"transcribe>ListTranscriptionJobs",
"transcribe>ListVocabularies",
"transcribe>ListVocabularyFilters",
"transfer:Describe*",
"transfer>List*",
"translate>List*",
"trustedadvisor:Describe*",
"waf-regional:GetWebACL",
"waf-regional>ListResourcesForWebACL",
"waf-regional>ListTagsForResource",
"waf-regional>ListWebACLs",
"waf:GetWebACL",
"waf>ListTagsForResource",
"waf>ListWebACLs",
"wafv2:GetWebACL",
"wafv2:GetWebACLForResource",
"wafv2>ListAvailableManagedRuleGroups",
"wafv2>ListIPSets",
"wafv2>ListLoggingConfigurations",
"wafv2>ListRegexPatternSets",
```

```

    "wafv2:ListResourcesForWebACL",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "wafv2:ListWebACLs",
    "workdocs:DescribeResourcePermissions",
    "workspaces:Describe*",
    "xray:GetEncryptionConfig",
    "xray:GetGroup",
    "xray:GetGroups",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetTraceSummaries",
    "xray:ListTagsForResource"
  ]
},
{
  "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"
  ]
}
]
}

```

## Saiba mais

- [Crie um conjunto de permissões ao utilizar as políticas gerenciadas pela AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade IAM](#)
- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## SecurityLakeServiceLinkedRole

SecurityLakeServiceLinkedRole é uma [política gerenciada pela AWS](#) que concede permissões para operar o serviço Amazon Security Lake em seu nome

## Utilização desta política

Essa política é vinculada a uma função associada a um serviço, o que possibilita que este serviço execute ações em seu próprio nome. Não é possível vincular esta política a usuários, grupos ou funções.

## Detalhes desta política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 29 de novembro de 2022, 14:03 UTC
- Horário editado: 29 de fevereiro de 2024, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões desta política. Quando um usuário ou função da política faz uma solicitação para acessar um AWS recurso, AWS verifica a versão padrão da política para determinar se a solicitação deve ser permitida.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
```

```
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeAccount"
    ],
    "Resource" : [
      "arn:aws:organizations::*:account/o-*/*"
    ]
  },
  {
    "Sid" : "AllowManagementOfServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail>DeleteServiceLinkedChannel",
      "cloudtrail:GetServiceLinkedChannel",
      "cloudtrail:UpdateServiceLinkedChannel"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
  },
  {
    "Sid" : "AllowListServiceLinkedChannel",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "DescribeAnyVpc",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ListDelegatedAdmins",
    "Effect" : "Allow",
    "Action" : [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
```

```
    "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
  }
}
},
{
  "Sid" : "AllowWafLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "wafv2:LogScope" : "SecurityLake"
    }
  }
},
{
  "Sid" : "AllowPutLoggingConfiguration",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutLoggingConfiguration"
  ],
  "Resource" : "*",
  "Condition" : {
    "ArnLike" : {
      "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
    }
  }
},
{
  "Sid" : "ListWebACLs",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:ListWebACLs"
  ],
  "Resource" : "*"
}
]
```

## Saiba mais

- [Compreenda o controle de versionamento das políticas do IAM](#)
- [Comece com políticas AWS gerenciadas e adote permissões com privilégios mínimos](#)

## ServerMigration\_ServiceRole

ServerMigration\_ServiceRole é uma [política AWS gerenciada](#) que: Permissões para permitir que o Serviço de Migração de AWS Servidores migre VMs para o EC2: permite que o Serviço de Migração de Servidores coloque os recursos migrados na conta EC2 do cliente.

### A utilização desta política

Você pode vincular a ServerMigration\_ServiceRole aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 11 de agosto de 2020, 20:41 UTC
- Horário editado: 15 de outubro de 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```

    "cloudformation:CreateChangeSet",
    "cloudformation:CreateStack"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**",
  "Condition" : {
    "Null" : {
      "cloudformation:ResourceTypes" : "false"
    },
    "ForAllValues:StringEquals" : {
      "cloudformation:ResourceTypes" : [
        "AWS::EC2::Instance",
        "AWS::ApplicationInsights::Application",
        "AWS::ResourceGroups::Group"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DeleteStack",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:DeleteChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudformation:GetTemplate"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/**"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",

```



```

    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::sms-app-*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "sms:CreateReplicationJob",
    "sms>DeleteReplicationJob",
    "sms:GetReplicationJobs",
    "sms:GetReplicationRuns",
    "sms:GetServers",
    "sms:ImportServerCatalog",
    "sms:StartOnDemandReplicationRun",
    "sms:UpdateReplicationJob"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ssm:*::document/AWS-RunRemoteScript",
    "arn:aws:s3:::sms-app-*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ssm:resourceTag/UseForSMSApplicationValidation" : [
        "true"
      ]
    }
  }
}

```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ssm:CancelCommand",
      "ssm:GetCommandInvocation"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CopySnapshot"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CopySnapshot",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifySnapshotAttribute",
      "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/SMSJobId" : [
          "sms-*"
        ]
      }
    }
  }
]
```

```

    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:CopyImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSnapshotAttribute",
    "ec2:DeregisterImage",
    "ec2:ImportImage",
    "ec2:DescribeImportImageTasks",
    "ec2:GetEbsEncryptionByDefault"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:GetInstanceProfile"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",

```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIfExists" : {
        "iam:PassedToService" : "cloudformation.amazonaws.com"
      },
      "StringLike" : {
        "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  }
]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServerMigrationConnector

ServerMigrationConnector é uma [política AWS gerenciada](#) que: Permissões para permitir que o AWS Server Migration Connector migre VMs para o EC2. Permite comunicação com o AWS Server Migration Service, acesso de leitura/gravação aos buckets do S3 começando com 'sms-b-' e 'import-to-ec2-', bem como aos buckets usados para atualização do Server Migration Connector, AWS registro do AWS Server Migration Connector e upload de métricas para. AWS AWS

## A utilização desta política

Você pode vincular a `ServerMigrationConnector` aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de outubro de 2016, 21:45 UTC
- Horário editado: 24 de outubro de 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutLifecycleConfiguration",
    "s3:AbortMultipartUpload",
    "s3:ListBucketMultipartUploads",
    "s3:ListMultipartUploadParts"
  ],
  "Resource" : [
    "arn:aws:s3:::sms-b-*",
    "arn:aws:s3:::import-to-ec2-*",
    "arn:aws:s3:::server-migration-service-upgrade",
    "arn:aws:s3:::server-migration-service-upgrade/*",
    "arn:aws:s3:::connector-platform-upgrade-info/*",
    "arn:aws:s3:::connector-platform-upgrade-info",
    "arn:aws:s3:::connector-platform-upgrade-bundles/*",
    "arn:aws:s3:::connector-platform-upgrade-bundles",
    "arn:aws:s3:::connector-platform-release-notes/*",
    "arn:aws:s3:::connector-platform-release-notes"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "awsconnector:*",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "SNS:Publish"
  ],
  "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServerMigrationServiceConsoleFullAccess

ServerMigrationServiceConsoleFullAccess é uma [política AWS gerenciada](#) que:  
Permissões necessárias para usar todos os recursos do Server Migration Service Console

### A utilização desta política

Você pode vincular a ServerMigrationServiceConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 09 de maio de 2020, 17:18 UTC
- Horário editado: 20 de julho de 2020, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
"Statement" : [
  {
    "Action" : [
      "sms:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "cloudformation:ListStacks",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackResources"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : "s3:ListAllMyBuckets",
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "arn:aws:s3:::sms-app-*/*"
  },
  {
    "Action" : [
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
  {
    "Action" : [
      "iam:ListRoles"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  },
],
```



```
{
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "sms.amazonaws.com"
    }
  },
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : "iam:GetInstanceProfile",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole é uma [política AWS gerenciada](#) que: Permissões para permitir que o Serviço de Migração de AWS Servidores crie e atualize AWS recursos relevantes para o cliente Conta da AWS para iniciar servidores e aplicativos migrados.

## A utilização desta política

Você pode vincular a ServerMigrationServiceLaunchRole aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 26 de novembro de 2018, 19:53 UTC
- Horário editado: 15 de outubro de 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
            "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
    "Resource" : "arn:aws:ec2:*:*:instance/*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DisassociateIamInstanceProfile",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances",
      "ec2:Describe*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*",
      "cloudformation:ListStackResources",
      "cloudformation:DescribeStacks"
    ],
    "Resource" : "*"
  }
```

```

    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights>DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights>DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups>DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam:*:*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  }
}

```

```
}  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServerMigrationServiceRoleForInstanceValidation

ServerMigrationServiceRoleForInstanceValidation é uma [política AWS gerenciada](#) que: Permissões para permitir que o AWS SMS execute o script de validação de dados usado e envie o script de sucesso/falha de volta ao SMS

### A utilização desta política

Você pode vincular a ServerMigrationServiceRoleForInstanceValidation aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 20 de julho de 2020, 22:25 UTC
- Horário editado: 20 de julho de 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServiceQuotasFullAccess

ServiceQuotasFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total às Service Quotas

## A utilização desta política

Você pode vincular a ServiceQuotasFullAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2019, 15:44 UTC
- Horário editado: 04 de fevereiro de 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

## Versão da política

Versão da política: v4 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
```

```
    "tag:GetTagValues",
    "servicequotas:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DeleteAlarms"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/ServiceQuotaMonitor" : "false"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "organizations:ServicePrincipal" : [
        "servicequotas.amazonaws.com"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "servicequotas.amazonaws.com"
    }
  }
}
]
```



```
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServiceQuotasReadOnlyAccess

ServiceQuotasReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura às Service Quotas

### A utilização desta política

Você pode vincular a ServiceQuotasReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 24 de junho de 2019, 15:31 UTC
- Horário editado: 21 de dezembro de 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAccountLimits",
      "cloudformation:DescribeAccountLimits",
      "cloudwatch:DescribeAlarmsForMetric",
      "cloudwatch:DescribeAlarms",
      "cloudwatch:GetMetricData",
      "cloudwatch:GetMetricStatistics",
      "dynamodb:DescribeLimits",
      "elasticloadbalancing:DescribeAccountLimits",
      "iam:GetAccountSummary",
      "kinesis:DescribeLimits",
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization",
      "rds:DescribeAccountAttributes",
      "route53:GetAccountLimit",
      "tag:GetTagKeys",
      "tag:GetTagValues",
      "servicequotas:GetAssociationForServiceQuotaTemplate",
      "servicequotas:GetAWSDefaultServiceQuota",
      "servicequotas:GetRequestedServiceQuotaChange",
      "servicequotas:GetServiceQuota",
      "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
      "servicequotas:ListAWSDefaultServiceQuotas",
      "servicequotas:ListRequestedServiceQuotaChangeHistory",
      "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
      "servicequotas:ListServices",
      "servicequotas:ListServiceQuotas",
      "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
      "servicequotas:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)

- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ServiceQuotasServiceRolePolicy

ServiceQuotasServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite que os Service Quotas criem casos de suporte em seu nome

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário da criação: 22 de maio de 2019, 20:44 UTC
- Horário editado: 24 de junho de 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

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

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## SimpleWorkflowFullAccess

SimpleWorkflowFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao serviço de configuração do Simple Workflow.

### A utilização desta política

Você pode vincular a SimpleWorkflowFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 06 de fevereiro de 2015, 18:41 UTC
- Horário editado: 06 de fevereiro de 2015, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/SimpleWorkflowFullAccess

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

### Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## SupportUser

SupportUser é uma [política AWS gerenciada](#) que: Essa política concede permissões para solucionar e resolver problemas em uma Conta da AWS. Essa política também permite que o usuário entre em contato com o AWS suporte para criar e gerenciar casos.

### A utilização desta política

Você pode vincular a SupportUser aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:21 UTC
- Horário editado: 25 de agosto de 2023, 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

## Versão da política

Versão da política: v8 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",

```

```
"codecommit:BatchGetRepositories",
"codecommit:Get*",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:AcknowledgeJob",
"codepipeline:AcknowledgeThirdPartyJob",
"codepipeline:ListActionTypes",
"codepipeline:ListPipelines",
"codepipeline:PollForJobs",
"codepipeline:PollForThirdPartyJobs",
"codepipeline:GetPipelineState",
"codepipeline:GetPipeline",
"cognito-identity:List*",
"cognito-identity:LookupDeveloperIdentity",
"cognito-identity:Describe*",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeRiskConfiguration",
"cognito-idp:DescribeUserImportJob",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:List*",
"cognito-sync:Describe*",
"cognito-sync:GetBulkPublishDetails",
"cognito-sync:GetCognitoEvents",
"cognito-sync:GetIdentityPoolConfiguration",
"cognito-sync:List*",
"config:DescribeConfigurationRecorders",
"config:DescribeConfigurationRecorderStatus",
"config:DescribeConfigRuleEvaluationStatus",
"config:DescribeConfigRules",
"config:DescribeDeliveryChannels",
"config:DescribeDeliveryChannelStatus",
"config:GetResourceConfigHistory",
"config:ListDiscoveredResources",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ReportTaskProgress",
"datapipeline:ReportTaskRunnerHeartbeat",
"devicefarm:List*",
```

```
"devicefarm:Get*",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:ListConfigurations",
"dms:Describe*",
"dms:List*",
"ds:DescribeDirectories",
"ds:DescribeSnapshots",
"ds:GetDirectoryLimits",
"ds:GetSnapshotLimits",
"ds:ListAuthorizedApplications",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"ec2:Describe*",
"ec2:DescribeHosts",
"ec2:describeIdentityIdFormat",
"ec2:DescribeIdFormat",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeNatGateways",
"ec2:DescribeReservedInstancesModifications",
"ec2:DescribeTags",
"ec2:SearchLocalGatewayRoutes",
"ecr:GetRepositoryPolicy",
"ecr:BatchCheckLayerAvailability",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:RequestEnvironmentInfo",
"elasticbeanstalk:RetrieveEnvironmentInfo",
"elasticbeanstalk:ValidateConfigurationSettings",
"elasticfilesystem:Describe*",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:List*",
"elastictranscoder:List*",
"elastictranscoder:ReadJob",
"elasticfilesystem:DescribeFileSystems",
```



```
"es:Describe*",
"es:List*",
"es:ESHttpGet",
"es:ESHttpHead",
"events:DescribeRule",
"events:List*",
"events:TestEventPattern",
"firehose:Describe*",
"firehose:List*",
"gamelift:List*",
"gamelift:Describe*",
"glacier:ListVaults",
"glacier:DescribeVault",
"glacier:DescribeJob",
"glacier:Get*",
"glacier:List*",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"importexport:GetStatus",
"importexport:ListJobs",
"inspector:Describe*",
"inspector:List*",
"iot:Describe*",
"iot:Get*",
"iot:List*",
"kinesisanalytics:DescribeApplication",
"kinesisanalytics:DiscoverInputSchema",
"kinesisanalytics:GetApplicationState",
"kinesisanalytics:ListApplications",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:List*",
"lambda:Get*",
"logs:Describe*",
"logs:TestMetricFilter",
"machinelearning:Describe*",
"machinelearning:Get*",
"opsworks:Describe*",
```

```
"rds:Describe*",
"rds:ListTagsForResource",
"redshift:Describe*",
"route53:Get*",
"route53:List*",
"route53domains:CheckDomainAvailability",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
"route53domains:List*",
"s3:List*",
"sdb:GetAttributes",
"sdb:List*",
"sdb:Select*",
"servicecatalog:SearchProducts",
"servicecatalog:DescribeProduct",
"servicecatalog:DescribeProductView",
"servicecatalog:ListLaunchPaths",
"servicecatalog:DescribeProvisioningParameters",
"servicecatalog:ListRecordHistory",
"servicecatalog:DescribeRecord",
"servicecatalog:ScanProvisionedProducts",
"ses:Get*",
"ses:List*",
"sns:Get*",
"sns:List*",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"sqs:ListQueues",
"sqs:ReceiveMessage",
"ssm:List*",
"ssm:Describe*",
"storagegateway:Describe*",
"storagegateway:List*",
"swf:Count*",
"swf:Describe*",
"swf:Get*",
"swf:List*",
"waf:Get*",
"waf:List*",
"workdocs:Describe*",
"workmail:Describe*",
"workmail:Get*",
"workspaces:Describe*"
],
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## SystemAdministrator

SystemAdministrator é uma [política AWS gerenciada](#) que: Concede as permissões de acesso total necessárias aos recursos necessários para operações de aplicativos e desenvolvimento.

### A utilização desta política

Você pode vincular a SystemAdministrator aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:23 UTC
- Horário editado: 24 de agosto de 2020, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

### Versão da política

Versão da política: v6 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
```

```
"ec2:Copy*",
"ec2:CreateCustomerGateway",
"ec2:CreateDhcpOptions",
"ec2:CreateFlowLogs",
"ec2:CreateImage",
"ec2:CreateInstanceExportTask",
"ec2:CreateInternetGateway",
"ec2:CreateKeyPair",
"ec2:CreateLaunchTemplate",
"ec2:CreateLaunchTemplateVersion",
"ec2:CreateNatGateway",
"ec2:CreateNetworkInterface",
"ec2:CreatePlacementGroup",
"ec2:CreateReservedInstancesListing",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateSpotDatafeedSubscription",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpnConnection",
"ec2:CreateVpnConnectionRoute",
"ec2:CreateVpnGateway",
"ec2>DeleteFlowLogs",
"ec2>DeleteKeyPair",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteLaunchTemplateVersions",
"ec2>DeleteNatGateway",
"ec2>DeleteNetworkInterface",
"ec2>DeletePlacementGroup",
"ec2>DeleteSnapshot",
"ec2>DeleteSpotDatafeedSubscription",
"ec2>DeleteSubnet",
"ec2>DeleteTags",
"ec2>DeleteVpc",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteVpnConnection",
"ec2>DeleteVpnConnectionRoute",
"ec2>DeleteVpnGateway",
"ec2:DeregisterImage",
```

```
"ec2:Describe*",
"ec2:DetachInternetGateway",
"ec2:DetachNetworkInterface",
"ec2:DetachVpnGateway",
"ec2:DisableVgwRoutePropagation",
"ec2:DisableVpcClassicLinkDnsSupport",
"ec2:DisassociateAddress",
"ec2:DisassociateRouteTable",
"ec2:EnableVgwRoutePropagation",
"ec2:EnableVolumeIO",
"ec2:EnableVpcClassicLinkDnsSupport",
"ec2:GetConsoleOutput",
"ec2:GetHostReservationPurchasePreview",
"ec2:GetLaunchTemplateData",
"ec2:GetPasswordData",
"ec2: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"
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## TranslateFullAccess

TranslateFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon Translate.

### A utilização desta política

Você pode vincular a TranslateFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 27 de novembro de 2018, 23:36 UTC
- Horário editado: 08 de janeiro de 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

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

```
{
  "Action" : [
    "translate:*",
    "comprehend:DetectDominantLanguage",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "iam:ListRoles",
    "iam:GetRole"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## TranslateReadOnly

TranslateReadOnly é uma [política AWS gerenciada](#) que: Fornece acesso somente para leitura ao Amazon Translate.

### A utilização desta política

Você pode vincular a TranslateReadOnly aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2017, 18:22 UTC

- Horário editado: 24 de maio de 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

## Versão da política

Versão da política: v7 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## ViewOnlyAccess

ViewOnlyAccess é uma [política AWS gerenciada](#) que: Essa política concede permissões para visualizar recursos e metadados básicos em todos os AWS serviços.

### A utilização desta política

Você pode vincular a ViewOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de trabalho
- Horário de criação: 10 de novembro de 2016, 17:20 UTC
- Horário editado: 06 de março de 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

### Versão da política

Versão da política: v17 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
```

```
"aws-marketplace:ViewSubscriptions",
"batch:ListJobs",
"clouddirectory:ListAppliedSchemaArns",
"clouddirectory:ListDevelopmentSchemaArns",
"clouddirectory:ListDirectories",
"clouddirectory:ListPublishedSchemaArns",
"cloudformation:DescribeStacks",
"cloudformation:List*",
"cloudfront:List*",
"cloudhsm:ListAvailableZones",
"cloudhsm:ListHapgs",
"cloudhsm:ListHsms",
"cloudhsm:ListLunaClients",
"cloudsearch:DescribeDomains",
"cloudsearch:List*",
"cloudtrail:DescribeTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"codebuild:ListBuilds*",
"codebuild:ListProjects",
"codecommit:List*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:ListPipelines",
"codestar:List*",
"cognito-identity:ListIdentities",
"cognito-identity:ListIdentityPools",
"cognito-idp:List*",
"cognito-sync:ListDatasets",
"config:Describe*",
"config:List*",
"connect:List*",
"comprehend:Describe*",
"comprehend:List*",
"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: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:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:DescribeAcceleratorOfferings",
"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*",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
```



```
"events:ListRuleNamesByTarget",
"events:ListRules",
"events:ListTargetsByRule",
"firehose:DescribeDeliveryStream",
"firehose:List*",
"fsx:DescribeFileSystems",
"gamelift:List*",
"glacier:List*",
"greengrass:List*",
"iam:GetAccountSummary",
"iam:GetLoginProfile",
"iam:List*",
"importexport:ListJobs",
"inspector:List*",
"iot:List*",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kms:ListKeys",
"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*",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"machinelearning:Describe*",
"mediacconnect:ListEntitlements",
"mediacconnect:ListFlows",
"mediacconnect:ListOfferings",
```

```
"mediaconnect:ListReservations",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetImportJobs",
"mobiletargeting:GetSegments",
"opsworks-cm:Describe*",
"opsworks:Describe*",
"organizations:List*",
"outposts:GetOutpost",
"outposts:GetOutpostInstanceTypes",
"outposts:ListOutposts",
"outposts:ListSites",
"outposts:ListTagsForResource",
"polly:Describe*",
"polly:List*",
"rds:Describe*",
"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",
"sagemaker:Describe*",
"sagemaker:List*",
"sdb:List*",
"servicecatalog:List*",
"ses:List*",
"shield:List*",
"sns:List*",
"sqs:ListQueues",
"ssm:ListAssociations",
"ssm:ListDocuments",
"states:ListActivities",
"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*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## VMImportExportRoleForAWSConnector

VMImportExportRoleForAWSConnector é uma [política AWS gerenciada que: Política](#) padrão para a função de serviço VM Import/Export, para clientes que usam o Connector. AWS O serviço VM Import/Export assume uma função com essa política para atender às solicitações de migração de máquinas virtuais do AWS dispositivo virtual Connector. (Observe que o AWS Connector usa a política gerenciada “AWSConnector” para emitir solicitações em nome do cliente para o serviço VM Import/Export.) Fornece a capacidade de criar AMIs e instantâneos do EBS, modificar atributos de instantâneos do EBS, fazer chamadas “Describe\*” em objetos do EC2 e ler os buckets do S3 começando com “importar para ec2”.

## A utilização desta política

Você pode vincular a `VMImportExportRoleForAWSConnector` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: Política de função de serviço
- Horário de criação: 03 de setembro de 2015, 20:48 UTC
- Horário editado: 03 de setembro de 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
    ],
    "Resource" : "*"
}
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## VPCLatticeFullAccess

VPCLatticeFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total ao Amazon VPC Lattice e acesso aos serviços de dependência.

### A utilização desta política

Você pode vincular a VPCLatticeFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de março de 2023, 02:49 UTC
- Horário editado: 30 de março de 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "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"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## VPCLatticeReadOnlyAccess

VPCLatticeReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura ao Amazon VPC Lattice por meio do AWS Management Console, e acesso limitado aos serviços de dependência.

### A utilização desta política

Você pode vincular a VPCLatticeReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de março de 2023, 02:47 UTC
- Horário editado: 30 de março de 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "vpc-lattice:Get*",
      "vpc-lattice:List*",
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "cloudwatch:GetMetricData",
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcAttribute",
      "ec2:DescribeVpcs",
      "elasticloadbalancing:DescribeLoadBalancers",
      "firehose:DescribeDeliveryStream",
      "firehose:ListDeliveryStreams",
      "lambda:ListAliases",
      "lambda:ListFunctions",
      "lambda:ListVersionsByFunction",
      "logs:DescribeLogGroups",
      "logs:GetLogDelivery",
      "logs:ListLogDeliveries",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

# VPCLatticeServicesInvokeAccess

VPCLatticeServicesInvokeAccess é uma [política AWS gerenciada](#) que: Fornece acesso à invocação de serviços do Amazon VPC Lattice.

## A utilização desta política

Você pode vincular a VPCLatticeServicesInvokeAccess aos seus usuários, grupos e perfis.

## Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 30 de março de 2023, 02:45 UTC
- Horário editado: 30 de março de 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WAFLoggingServiceRolePolicy

WAFLoggingServiceRolePolicy é uma [política AWS gerenciada](#) que: Criar SLR para gravar os registros do cliente em um fluxo de bombehose

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de agosto de 2018, 21:05 UTC
- Horário editado: 24 de agosto de 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
    ]
  }
]
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WAFRegionalLoggingServiceRolePolicy

WAFRegionalLoggingServiceRolePolicy é uma [política AWS gerenciada](#) que: Criar SLR para gravar os registros do cliente em um fluxo de bombehose

### A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 24 de agosto de 2018, 18:40 UTC
- Horário editado: 24 de agosto de 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

## Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WAFV2LoggingServiceRolePolicy

WAFV2LoggingServiceRolePolicy é uma [política AWS gerenciada](#) que: Essa política cria uma função vinculada ao serviço que permite ao AWS WAF gravar registros no Amazon Kinesis Data Firehose.

## A utilização desta política

Essa política é vinculada a uma função associada a um serviço, que possibilita que o serviço execute ações em seu próprio nome. Não é possível vincular essa política a usuários, grupos ou funções.

### Detalhes da política

- Tipo: Política de função vinculada ao serviço
- Horário de criação: 07 de novembro de 2019, 00:40 UTC
- Horário editado: 23 de julho de 2020, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

### Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

## Saiba mais

- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WellArchitectedConsoleFullAccess

WellArchitectedConsoleFullAccess é uma [política AWS gerenciada](#) que: Fornece acesso total à AWS Well-Architected Tool por meio do AWS Management Console

### A utilização desta política

Você pode vincular a WellArchitectedConsoleFullAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2018, 18:19 UTC
- Horário editado: 29 de novembro de 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
```

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WellArchitectedConsoleReadOnlyAccess

WellArchitectedConsoleReadOnlyAccess é uma [política AWS gerenciada](#) que: Fornece acesso somente de leitura à Well-Architected Tool AWS por meio do AWS Management Console

### A utilização desta política

Você pode vincular a WellArchitectedConsoleReadOnlyAccess aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Horário de criação: 29 de novembro de 2018, 18:21 UTC
- Horário editado: 29 de junho de 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`



## Versão da política

Versão da política: v2 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

## Documento da política JSON

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

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

## WorkLinkServiceRolePolicy

WorkLinkServiceRolePolicy é uma [política AWS gerenciada](#) que: Permite o acesso Serviços da AWS e os recursos usados ou gerenciados pelo Amazon WorkLink

## A utilização desta política

Você pode vincular a `WorkLinkServiceRolePolicy` aos seus usuários, grupos e perfis.

### Detalhes da política

- Tipo: política gerenciada da AWS
- Hora da criação: 23 de janeiro de 2019, 19:03 UTC
- Horário editado: 23 de janeiro de 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

### Versão da política

Versão da política: v1 (padrão)

A versão padrão da política é aquela que define as permissões para a política. Quando um usuário ou função com essa política faz uma solicitação para acessar um atributo AWS, AWS verifica a versão padrão da política para determinar se concede a permissão solicitada.

### Documento da política JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"  
  }  
]  
}
```

## Saiba mais

- [Crie um conjunto de permissões usando políticas gerenciadas da AWS no IAM Identity Center](#)
- [Adicionar e remover permissões de identidade do IAM](#)
- [Entenda o controle de versionamento das políticas do IAM](#)
- [Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo](#)

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.