



リファレンスガイド

AWS 管理ポリシー



AWS 管理ポリシー: リファレンスガイド

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

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない他の商標はすべてそれぞれの所有者に帰属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon の支援を受けているとはかぎりません。

Table of Contents

AWS マネージドポリシーとは何ですか？	1
ポリシーリファレンスページについて	1
非推奨の AWS マネージドポリシー	2
AWS マネージドポリシー	3
AccessAnalyzerServiceRolePolicy	44
このポリシーを使用すると	44
ポリシーの詳細	44
ポリシーのバージョン	44
JSON ポリシードキュメント	45
詳細はこちら	47
AdministratorAccess	47
このポリシーを使用すると	47
ポリシーの詳細	47
ポリシーのバージョン	48
JSON ポリシードキュメント	48
詳細はこちら	48
AdministratorAccess-Amplify	48
このポリシーを使用すると	48
ポリシーの詳細	49
ポリシーのバージョン	49
JSON ポリシードキュメント	49
詳細はこちら	59
AdministratorAccess-AWSElasticBeanstalk	60
このポリシーを使用すると	60
ポリシーの詳細	60
ポリシーのバージョン	60
JSON ポリシードキュメント	60
詳細はこちら	68
AlexaForBusinessDeviceSetup	69
このポリシーを使用すると	69
ポリシーの詳細	69
ポリシーのバージョン	69
JSON ポリシードキュメント	69
詳細はこちら	70

AlexaForBusinessFullAccess	70
このポリシーを使用すると	70
ポリシーの詳細	70
ポリシーのバージョン	71
JSON ポリシードキュメント	71
詳細はこちら	72
AlexaForBusinessGatewayExecution	72
このポリシーを使用すると	73
ポリシーの詳細	73
ポリシーのバージョン	73
JSON ポリシードキュメント	73
詳細はこちら	74
AlexaForBusinessLifesizeDelegatedAccessPolicy	74
このポリシーを使用すると	74
ポリシーの詳細	74
ポリシーのバージョン	75
JSON ポリシードキュメント	75
詳細はこちら	77
AlexaForBusinessNetworkProfileServicePolicy	77
このポリシーを使用すると	78
ポリシーの詳細	78
ポリシーのバージョン	78
JSON ポリシードキュメント	78
詳細はこちら	79
AlexaForBusinessPolyDelegatedAccessPolicy	79
このポリシーを使用すると	79
ポリシーの詳細	79
ポリシーのバージョン	79
JSON ポリシードキュメント	80
詳細はこちら	81
AlexaForBusinessReadOnlyAccess	82
このポリシーを使用すると	82
ポリシーの詳細	82
ポリシーのバージョン	82
JSON ポリシードキュメント	82
詳細はこちら	83

AmazonAPIGatewayAdministrator	83
このポリシーを使用すると	83
ポリシーの詳細	83
ポリシーのバージョン	83
JSON ポリシードキュメント	84
詳細はこちら	84
AmazonAPIGatewayInvokeFullAccess	84
このポリシーを使用すると	84
ポリシーの詳細	84
ポリシーのバージョン	85
JSON ポリシードキュメント	85
詳細はこちら	85
AmazonAPIGatewayPushToCloudWatchLogs	85
このポリシーを使用すると	86
ポリシーの詳細	86
ポリシーのバージョン	86
JSON ポリシードキュメント	86
詳細はこちら	87
AmazonAppFlowFullAccess	87
このポリシーを使用すると	87
ポリシーの詳細	87
ポリシーのバージョン	87
JSON ポリシードキュメント	88
詳細はこちら	90
AmazonAppFlowReadOnlyAccess	91
このポリシーを使用すると	91
ポリシーの詳細	91
ポリシーのバージョン	91
JSON ポリシードキュメント	91
詳細はこちら	92
AmazonAppStreamFullAccess	92
このポリシーを使用すると	92
ポリシーの詳細	92
ポリシーのバージョン	92
JSON ポリシードキュメント	93
詳細はこちら	94

AmazonAppStreamPCAAccess	95
このポリシーを使用すると	95
ポリシーの詳細	95
ポリシーのバージョン	95
JSON ポリシードキュメント	95
詳細はこちら	96
AmazonAppStreamReadOnlyAccess	96
このポリシーを使用すると	96
ポリシーの詳細	96
ポリシーのバージョン	97
JSON ポリシードキュメント	97
詳細はこちら	97
AmazonAppStreamServiceAccess	97
このポリシーを使用すると	98
ポリシーの詳細	98
ポリシーのバージョン	98
JSON ポリシードキュメント	98
詳細はこちら	99
AmazonAthenaFullAccess	99
このポリシーを使用すると	100
ポリシーの詳細	100
ポリシーのバージョン	100
JSON ポリシードキュメント	100
詳細はこちら	103
AmazonAugmentedAIFullAccess	104
このポリシーを使用すると	104
ポリシーの詳細	104
ポリシーのバージョン	104
JSON ポリシードキュメント	104
詳細はこちら	105
AmazonAugmentedAIHumanLoopFullAccess	106
このポリシーを使用すると	106
ポリシーの詳細	106
ポリシーのバージョン	106
JSON ポリシードキュメント	106
詳細はこちら	107

AmazonAugmentedAllIntegratedAPIAccess	107
このポリシーを使用すると	107
ポリシーの詳細	107
ポリシーのバージョン	107
JSON ポリシードキュメント	108
詳細はこちら	109
AmazonBedrockFullAccess	109
このポリシーを使用すると	109
ポリシーの詳細	109
ポリシーのバージョン	110
JSON ポリシードキュメント	110
詳細はこちら	111
AmazonBedrockReadOnly	111
このポリシーを使用すると	111
ポリシーの詳細	111
ポリシーのバージョン	112
JSON ポリシードキュメント	112
詳細はこちら	112
AmazonBraketFullAccess	113
このポリシーを使用すると	113
ポリシーの詳細	113
ポリシーのバージョン	113
JSON ポリシードキュメント	113
詳細はこちら	117
AmazonBraketJobsExecutionPolicy	118
このポリシーを使用すると	118
ポリシーの詳細	118
ポリシーのバージョン	118
JSON ポリシードキュメント	118
詳細はこちら	121
AmazonBraketServiceRolePolicy	121
このポリシーを使用すると	121
ポリシーの詳細	121
ポリシーのバージョン	121
JSON ポリシードキュメント	122
詳細はこちら	122

AmazonChimeFullAccess	123
このポリシーを使用すると	123
ポリシーの詳細	123
ポリシーのバージョン	123
JSON ポリシードキュメント	123
詳細はこちら	125
AmazonChimeReadOnly	126
このポリシーを使用すると	126
ポリシーの詳細	126
ポリシーのバージョン	126
JSON ポリシードキュメント	126
詳細はこちら	127
AmazonChimeSDK	127
このポリシーを使用すると	127
ポリシーの詳細	127
ポリシーのバージョン	127
JSON ポリシードキュメント	128
詳細はこちら	129
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy	129
このポリシーを使用すると	129
ポリシーの詳細	129
ポリシーのバージョン	129
JSON ポリシードキュメント	130
詳細はこちら	131
AmazonChimeSDKMessagingServiceRolePolicy	131
このポリシーを使用すると	131
ポリシーの詳細	131
ポリシーのバージョン	132
JSON ポリシードキュメント	132
詳細はこちら	133
AmazonChimeServiceRolePolicy	133
このポリシーを使用すると	133
ポリシーの詳細	133
ポリシーのバージョン	133
JSON ポリシードキュメント	133
詳細はこちら	134

AmazonChimeTranscriptionServiceLinkedRolePolicy	134
このポリシーを使用すると	134
ポリシーの詳細	134
ポリシーのバージョン	135
JSON ポリシードキュメント	135
詳細はこちら	135
AmazonChimeUserManagement	135
このポリシーを使用すると	136
ポリシーの詳細	136
ポリシーのバージョン	136
JSON ポリシードキュメント	136
詳細はこちら	137
AmazonChimeVoiceConnectorServiceLinkedRolePolicy	137
このポリシーを使用すると	138
ポリシーの詳細	138
ポリシーのバージョン	138
JSON ポリシードキュメント	138
詳細はこちら	140
AmazonCloudDirectoryFullAccess	140
このポリシーを使用すると	140
ポリシーの詳細	140
ポリシーのバージョン	141
JSON ポリシードキュメント	141
詳細はこちら	141
AmazonCloudDirectoryReadOnlyAccess	141
このポリシーを使用すると	142
ポリシーの詳細	142
ポリシーのバージョン	142
JSON ポリシードキュメント	142
詳細はこちら	143
AmazonCloudWatchEvidentlyFullAccess	143
このポリシーを使用すると	143
ポリシーの詳細	143
ポリシーのバージョン	143
JSON ポリシードキュメント	144
詳細はこちら	146

AmazonCloudWatchEvidentlyReadOnlyAccess	146
このポリシーを使用すると	146
ポリシーの詳細	146
ポリシーのバージョン	147
JSON ポリシードキュメント	147
詳細はこちら	147
AmazonCloudWatchEvidentlyServiceRolePolicy	148
このポリシーを使用すると	148
ポリシーの詳細	148
ポリシーのバージョン	148
JSON ポリシードキュメント	148
詳細はこちら	150
AmazonCloudWatchRUMFullAccess	150
このポリシーを使用すると	150
ポリシーの詳細	150
ポリシーのバージョン	150
JSON ポリシードキュメント	151
詳細はこちら	153
AmazonCloudWatchRUMReadOnlyAccess	153
このポリシーを使用すると	153
ポリシーの詳細	153
ポリシーのバージョン	154
JSON ポリシードキュメント	154
詳細はこちら	154
AmazonCloudWatchRUMServiceRolePolicy	155
このポリシーを使用すると	155
ポリシーの詳細	155
ポリシーのバージョン	155
JSON ポリシードキュメント	155
詳細はこちら	156
AmazonCodeCatalystFullAccess	156
このポリシーを使用すると	156
ポリシーの詳細	156
ポリシーのバージョン	157
JSON ポリシードキュメント	157
詳細はこちら	158

AmazonCodeCatalystReadOnlyAccess	158
このポリシーを使用すると	158
ポリシーの詳細	158
ポリシーのバージョン	158
JSON ポリシードキュメント	159
詳細はこちら	159
AmazonCodeCatalystSupportAccess	159
このポリシーを使用すると	159
ポリシーの詳細	159
ポリシーのバージョン	160
JSON ポリシードキュメント	160
詳細はこちら	161
AmazonCodeGuruProfilerAgentAccess	161
このポリシーを使用すると	161
ポリシーの詳細	161
ポリシーのバージョン	161
JSON ポリシードキュメント	161
詳細はこちら	162
AmazonCodeGuruProfilerFullAccess	162
このポリシーを使用すると	162
ポリシーの詳細	162
ポリシーのバージョン	163
JSON ポリシードキュメント	163
詳細はこちら	163
AmazonCodeGuruProfilerReadOnlyAccess	164
このポリシーを使用すると	164
ポリシーの詳細	164
ポリシーのバージョン	164
JSON ポリシードキュメント	164
詳細はこちら	165
AmazonCodeGuruReviewerFullAccess	165
このポリシーを使用すると	165
ポリシーの詳細	165
ポリシーのバージョン	166
JSON ポリシードキュメント	166
詳細はこちら	168

AmazonCodeGuruReviewerReadOnlyAccess	168
このポリシーを使用すると	169
ポリシーの詳細	169
ポリシーのバージョン	169
JSON ポリシードキュメント	169
詳細はこちら	170
AmazonCodeGuruReviewerServiceRolePolicy	170
このポリシーを使用すると	170
ポリシーの詳細	170
ポリシーのバージョン	170
JSON ポリシードキュメント	171
詳細はこちら	173
AmazonCodeGuruSecurityFullAccess	173
このポリシーを使用すると	173
ポリシーの詳細	173
ポリシーのバージョン	173
JSON ポリシードキュメント	173
詳細はこちら	174
AmazonCodeGuruSecurityScanAccess	174
このポリシーを使用すると	174
ポリシーの詳細	174
ポリシーのバージョン	174
JSON ポリシードキュメント	175
詳細はこちら	175
AmazonCognitoDeveloperAuthenticatedIdentities	175
このポリシーを使用すると	176
ポリシーの詳細	176
ポリシーのバージョン	176
JSON ポリシードキュメント	176
詳細はこちら	177
AmazonCognitoIamEmailServiceRolePolicy	177
このポリシーを使用すると	177
ポリシーの詳細	177
ポリシーのバージョン	177
JSON ポリシードキュメント	178
詳細はこちら	178

AmazonCognitoDpServiceRolePolicy	178
このポリシーを使用すると	178
ポリシーの詳細	179
ポリシーのバージョン	179
JSON ポリシードキュメント	179
詳細はこちら	179
AmazonCognitoPowerUser	180
このポリシーを使用すると	180
ポリシーの詳細	180
ポリシーのバージョン	180
JSON ポリシードキュメント	180
詳細はこちら	182
AmazonCognitoReadOnly	182
このポリシーを使用すると	182
ポリシーの詳細	182
ポリシーのバージョン	182
JSON ポリシードキュメント	182
詳細はこちら	183
AmazonCognitoUnAuthedIdentitiesSessionPolicy	183
このポリシーを使用すると	184
ポリシーの詳細	184
ポリシーのバージョン	184
JSON ポリシードキュメント	184
詳細はこちら	185
AmazonCognitoUnauthenticatedIdentities	185
このポリシーを使用すると	185
ポリシーの詳細	185
ポリシーのバージョン	186
JSON ポリシードキュメント	186
詳細はこちら	186
AmazonConnect_FullAccess	186
このポリシーを使用すると	186
ポリシーの詳細	187
ポリシーのバージョン	187
JSON ポリシードキュメント	187
詳細はこちら	190

AmazonConnectCampaignsServiceLinkedRolePolicy	190
このポリシーを使用すると	190
ポリシーの詳細	190
ポリシーのバージョン	190
JSON ポリシードキュメント	191
詳細はこちら	191
AmazonConnectReadOnlyAccess	191
このポリシーを使用すると	191
ポリシーの詳細	191
ポリシーのバージョン	192
JSON ポリシードキュメント	192
詳細はこちら	192
AmazonConnectServiceLinkedRolePolicy	193
このポリシーを使用すると	193
ポリシーの詳細	193
ポリシーのバージョン	193
JSON ポリシードキュメント	193
詳細はこちら	199
AmazonConnectSynchronizationServiceRolePolicy	199
このポリシーを使用すると	199
ポリシーの詳細	199
ポリシーのバージョン	199
JSON ポリシードキュメント	200
詳細はこちら	202
AmazonConnectVoiceIDFullAccess	202
このポリシーを使用すると	202
ポリシーの詳細	202
ポリシーのバージョン	202
JSON ポリシードキュメント	202
詳細はこちら	203
AmazonDataZoneDomainExecutionRolePolicy	203
このポリシーを使用すると	203
ポリシーの詳細	203
ポリシーのバージョン	203
JSON ポリシードキュメント	204
詳細はこちら	206

AmazonDataZoneEnvironmentRolePermissionsBoundary	207
このポリシーを使用すると	207
ポリシーの詳細	207
ポリシーのバージョン	207
JSON ポリシードキュメント	207
詳細はこちら	220
AmazonDataZoneFullAccess	220
このポリシーを使用すると	221
ポリシーの詳細	221
ポリシーのバージョン	221
JSON ポリシードキュメント	221
詳細はこちら	225
AmazonDataZoneFullUserAccess	225
このポリシーを使用すると	225
ポリシーの詳細	225
ポリシーのバージョン	225
JSON ポリシードキュメント	225
詳細はこちら	228
AmazonDataZoneGlueManageAccessRolePolicy	229
このポリシーを使用すると	229
ポリシーの詳細	229
ポリシーのバージョン	229
JSON ポリシードキュメント	229
詳細はこちら	234
AmazonDataZonePortalFullAccessPolicy	234
このポリシーを使用すると	235
ポリシーの詳細	235
ポリシーのバージョン	235
JSON ポリシードキュメント	235
詳細はこちら	235
AmazonDataZonePreviewConsoleFullAccess	236
このポリシーを使用すると	236
ポリシーの詳細	236
ポリシーのバージョン	236
JSON ポリシードキュメント	236
詳細はこちら	238

AmazonDataZoneProjectDeploymentPermissionsBoundary	238
このポリシーを使用すると	239
ポリシーの詳細	239
ポリシーのバージョン	239
JSON ポリシードキュメント	239
詳細はこちら	247
AmazonDataZoneProjectRolePermissionsBoundary	247
このポリシーを使用すると	247
ポリシーの詳細	248
ポリシーのバージョン	248
JSON ポリシードキュメント	248
詳細はこちら	255
AmazonDataZoneRedshiftGlueProvisioningPolicy	255
このポリシーを使用すると	256
ポリシーの詳細	256
ポリシーのバージョン	256
JSON ポリシードキュメント	256
詳細はこちら	264
AmazonDataZoneRedshiftManageAccessRolePolicy	264
このポリシーを使用すると	264
ポリシーの詳細	264
ポリシーのバージョン	265
JSON ポリシードキュメント	265
詳細はこちら	267
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary	267
このポリシーを使用すると	267
ポリシーの詳細	267
ポリシーのバージョン	268
JSON ポリシードキュメント	268
詳細はこちら	295
AmazonDataZoneSageMakerManageAccessRolePolicy	295
このポリシーを使用すると	295
ポリシーの詳細	296
ポリシーのバージョン	296
JSON ポリシードキュメント	296
詳細はこちら	301

AmazonDataZoneSageMakerProvisioningRolePolicy	301
このポリシーを使用すると	301
ポリシーの詳細	301
ポリシーのバージョン	301
JSON ポリシードキュメント	302
詳細はこちら	306
AmazonDetectiveFullAccess	306
このポリシーを使用すると	307
ポリシーの詳細	307
ポリシーのバージョン	307
JSON ポリシードキュメント	307
詳細はこちら	308
AmazonDetectiveInvestigatorAccess	308
このポリシーを使用すると	308
ポリシーの詳細	309
ポリシーのバージョン	309
JSON ポリシードキュメント	309
詳細はこちら	310
AmazonDetectiveMemberAccess	311
このポリシーを使用すると	311
ポリシーの詳細	311
ポリシーのバージョン	311
JSON ポリシードキュメント	311
詳細はこちら	312
AmazonDetectiveOrganizationsAccess	312
このポリシーを使用すると	312
ポリシーの詳細	312
ポリシーのバージョン	313
JSON ポリシードキュメント	313
詳細はこちら	314
AmazonDetectiveServiceLinkedRolePolicy	315
このポリシーを使用すると	315
ポリシーの詳細	315
ポリシーのバージョン	315
JSON ポリシードキュメント	315
詳細はこちら	316

AmazonDevOpsGuruConsoleFullAccess	316
このポリシーを使用すると	316
ポリシーの詳細	316
ポリシーのバージョン	316
JSON ポリシードキュメント	317
詳細はこちら	319
AmazonDevOpsGuruFullAccess	319
このポリシーを使用すると	319
ポリシーの詳細	320
ポリシーのバージョン	320
JSON ポリシードキュメント	320
詳細はこちら	322
AmazonDevOpsGuruOrganizationsAccess	322
このポリシーを使用すると	323
ポリシーの詳細	323
ポリシーのバージョン	323
JSON ポリシードキュメント	323
詳細はこちら	324
AmazonDevOpsGuruReadOnlyAccess	325
このポリシーを使用すると	325
ポリシーの詳細	325
ポリシーのバージョン	325
JSON ポリシードキュメント	325
詳細はこちら	327
AmazonDevOpsGuruServiceRolePolicy	327
このポリシーを使用すると	327
ポリシーの詳細	328
ポリシーのバージョン	328
JSON ポリシードキュメント	328
詳細はこちら	332
AmazonDMSCloudWatchLogsRole	332
このポリシーを使用すると	332
ポリシーの詳細	332
ポリシーのバージョン	333
JSON ポリシードキュメント	333
詳細はこちら	334

AmazonDMSRedshiftS3Role	334
このポリシーを使用すると	335
ポリシーの詳細	335
ポリシーのバージョン	335
JSON ポリシードキュメント	335
詳細はこちら	336
AmazonDMSVPCManagementRole	336
このポリシーを使用すると	336
ポリシーの詳細	336
ポリシーのバージョン	336
JSON ポリシードキュメント	337
詳細はこちら	337
AmazonDocDB-ElasticServiceRolePolicy	337
このポリシーを使用すると	338
ポリシーの詳細	338
ポリシーのバージョン	338
JSON ポリシードキュメント	338
詳細はこちら	339
AmazonDocDBConsoleFullAccess	339
このポリシーを使用すると	339
ポリシーの詳細	339
ポリシーのバージョン	339
JSON ポリシードキュメント	340
詳細はこちら	344
AmazonDocDBElasticFullAccess	344
このポリシーを使用すると	344
ポリシーの詳細	344
ポリシーのバージョン	344
JSON ポリシードキュメント	345
詳細はこちら	347
AmazonDocDBElasticReadOnlyAccess	348
このポリシーを使用すると	348
ポリシーの詳細	348
ポリシーのバージョン	348
JSON ポリシードキュメント	348
詳細はこちら	349

AmazonDocDBFullAccess	349
このポリシーを使用すると	349
ポリシーの詳細	350
ポリシーのバージョン	350
JSON ポリシードキュメント	350
詳細はこちら	353
AmazonDocDBReadOnlyAccess	353
このポリシーを使用すると	353
ポリシーの詳細	353
ポリシーのバージョン	353
JSON ポリシードキュメント	354
詳細はこちら	355
AmazonDRSVPCManagement	356
このポリシーを使用すると	356
ポリシーの詳細	356
ポリシーのバージョン	356
JSON ポリシードキュメント	356
詳細はこちら	357
AmazonDynamoDBFullAccess	357
このポリシーを使用すると	357
ポリシーの詳細	357
ポリシーのバージョン	358
JSON ポリシードキュメント	358
詳細はこちら	360
AmazonDynamoDBFullAccesswithDataPipeline	361
このポリシーを使用すると	361
ポリシーの詳細	361
ポリシーのバージョン	361
JSON ポリシードキュメント	361
詳細はこちら	363
AmazonDynamoDBReadOnlyAccess	364
このポリシーを使用すると	364
ポリシーの詳細	364
ポリシーのバージョン	364
JSON ポリシードキュメント	364
詳細はこちら	366

AmazonEBSCSIDriverPolicy	366
このポリシーを使用すると	366
ポリシーの詳細	366
ポリシーのバージョン	367
JSON ポリシードキュメント	367
詳細はこちら	370
AmazonEC2ContainerRegistryFullAccess	370
このポリシーを使用すると	370
ポリシーの詳細	370
ポリシーのバージョン	371
JSON ポリシードキュメント	371
詳細はこちら	371
AmazonEC2ContainerRegistryPowerUser	372
このポリシーを使用すると	372
ポリシーの詳細	372
ポリシーのバージョン	372
JSON ポリシードキュメント	372
詳細はこちら	373
AmazonEC2ContainerRegistryReadOnly	373
このポリシーを使用すると	373
ポリシーの詳細	374
ポリシーのバージョン	374
JSON ポリシードキュメント	374
詳細はこちら	375
AmazonEC2ContainerServiceAutoscaleRole	375
このポリシーを使用すると	375
ポリシーの詳細	375
ポリシーのバージョン	375
JSON ポリシードキュメント	375
詳細はこちら	376
AmazonEC2ContainerServiceEventsRole	376
このポリシーを使用すると	377
ポリシーの詳細	377
ポリシーのバージョン	377
JSON ポリシードキュメント	377
詳細はこちら	378

AmazonEC2ContainerServiceforEC2Role	378
このポリシーを使用すると	378
ポリシーの詳細	379
ポリシーのバージョン	379
JSON ポリシードキュメント	379
詳細はこちら	380
AmazonEC2ContainerServiceRole	380
このポリシーを使用すると	380
ポリシーの詳細	380
ポリシーのバージョン	381
JSON ポリシードキュメント	381
詳細はこちら	381
AmazonEC2FullAccess	382
このポリシーを使用すると	382
ポリシーの詳細	382
ポリシーのバージョン	382
JSON ポリシードキュメント	382
詳細はこちら	383
AmazonEC2ReadOnlyAccess	383
このポリシーを使用すると	384
ポリシーの詳細	384
ポリシーのバージョン	384
JSON ポリシードキュメント	384
詳細はこちら	385
AmazonEC2RoleforAWSCodeDeploy	385
このポリシーを使用すると	385
ポリシーの詳細	385
ポリシーのバージョン	386
JSON ポリシードキュメント	386
詳細はこちら	386
AmazonEC2RoleforAWSCodeDeployLimited	386
このポリシーを使用すると	387
ポリシーの詳細	387
ポリシーのバージョン	387
JSON ポリシードキュメント	387
詳細はこちら	388

AmazonEC2RoleforDataPipelineRole	388
このポリシーを使用すると	388
ポリシーの詳細	388
ポリシーのバージョン	389
JSON ポリシードキュメント	389
詳細はこちら	389
AmazonEC2RoleforSSM	390
このポリシーを使用すると	390
ポリシーの詳細	390
ポリシーのバージョン	390
JSON ポリシードキュメント	390
詳細はこちら	393
AmazonEC2RolePolicyForLaunchWizard	393
このポリシーを使用すると	393
ポリシーの詳細	393
ポリシーのバージョン	393
JSON ポリシードキュメント	394
詳細はこちら	397
AmazonEC2SpotFleetAutoscaleRole	398
このポリシーを使用すると	398
ポリシーの詳細	398
ポリシーのバージョン	398
JSON ポリシードキュメント	398
詳細はこちら	399
AmazonEC2SpotFleetTaggingRole	399
このポリシーを使用すると	400
ポリシーの詳細	400
ポリシーのバージョン	400
JSON ポリシードキュメント	400
詳細はこちら	401
AmazonECS_FullAccess	402
このポリシーを使用すると	402
ポリシーの詳細	402
ポリシーのバージョン	402
JSON ポリシードキュメント	402
詳細はこちら	408

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity	408
このポリシーを使用すると	408
ポリシーの詳細	408
ポリシーのバージョン	408
JSON ポリシードキュメント	409
詳細はこちら	411
AmazonECSInfrastructureRolePolicyForVolumes	411
このポリシーを使用すると	411
ポリシーの詳細	411
ポリシーのバージョン	411
JSON ポリシードキュメント	412
詳細はこちら	414
AmazonECSServiceRolePolicy	414
このポリシーを使用すると	414
ポリシーの詳細	414
ポリシーのバージョン	414
JSON ポリシードキュメント	414
詳細はこちら	419
AmazonECSTaskExecutionRolePolicy	419
このポリシーを使用すると	420
ポリシーの詳細	420
ポリシーのバージョン	420
JSON ポリシードキュメント	420
詳細はこちら	421
AmazonEFSCSIDriverPolicy	421
このポリシーを使用すると	421
ポリシーの詳細	421
ポリシーのバージョン	421
JSON ポリシードキュメント	421
詳細はこちら	423
AmazonEKS_CNI_Policy	423
このポリシーを使用すると	423
ポリシーの詳細	424
ポリシーのバージョン	424
JSON ポリシードキュメント	424
詳細はこちら	425

AmazonEKSClusterPolicy	425
このポリシーを使用すると	425
ポリシーの詳細	425
ポリシーのバージョン	426
JSON ポリシードキュメント	426
詳細はこちら	428
AmazonEKSConectorServiceRolePolicy	428
このポリシーを使用すると	428
ポリシーの詳細	428
ポリシーのバージョン	428
JSON ポリシードキュメント	429
詳細はこちら	430
AmazonEKSFargatePodExecutionRolePolicy	431
このポリシーを使用すると	431
ポリシーの詳細	431
ポリシーのバージョン	431
JSON ポリシードキュメント	431
詳細はこちら	432
AmazonEKSFForFargateServiceRolePolicy	432
このポリシーを使用すると	432
ポリシーの詳細	432
ポリシーのバージョン	432
JSON ポリシードキュメント	433
詳細はこちら	433
AmazonEKSLocalOutpostClusterPolicy	433
このポリシーを使用すると	434
ポリシーの詳細	434
ポリシーのバージョン	434
JSON ポリシードキュメント	434
詳細はこちら	436
AmazonEKSLocalOutpostServiceRolePolicy	436
このポリシーを使用すると	436
ポリシーの詳細	436
ポリシーのバージョン	437
JSON ポリシードキュメント	437
詳細はこちら	442

AmazonEKSServicePolicy	443
このポリシーを使用すると	443
ポリシーの詳細	443
ポリシーのバージョン	443
JSON ポリシードキュメント	443
詳細はこちら	445
AmazonEKSServiceRolePolicy	445
このポリシーを使用すると	445
ポリシーの詳細	445
ポリシーのバージョン	446
JSON ポリシードキュメント	446
詳細はこちら	448
AmazonEKSVPCResourceController	448
このポリシーを使用すると	448
ポリシーの詳細	448
ポリシーのバージョン	449
JSON ポリシードキュメント	449
詳細はこちら	450
AmazonEKSWorkerNodePolicy	450
このポリシーを使用すると	450
ポリシーの詳細	450
ポリシーのバージョン	450
JSON ポリシードキュメント	450
詳細はこちら	451
AmazonElastiCacheFullAccess	451
このポリシーを使用すると	451
ポリシーの詳細	452
ポリシーのバージョン	452
JSON ポリシードキュメント	452
詳細はこちら	455
AmazonElastiCacheReadOnlyAccess	455
このポリシーを使用すると	456
ポリシーの詳細	456
ポリシーのバージョン	456
JSON ポリシードキュメント	456
詳細はこちら	456

AmazonElasticContainerRegistryPublicFullAccess	457
このポリシーを使用すると	457
ポリシーの詳細	457
ポリシーのバージョン	457
JSON ポリシードキュメント	457
詳細はこちら	458
AmazonElasticContainerRegistryPublicPowerUser	458
このポリシーを使用すると	458
ポリシーの詳細	458
ポリシーのバージョン	459
JSON ポリシードキュメント	459
詳細はこちら	459
AmazonElasticContainerRegistryPublicReadOnly	460
このポリシーを使用すると	460
ポリシーの詳細	460
ポリシーのバージョン	460
JSON ポリシードキュメント	460
詳細はこちら	461
AmazonElasticFileSystemClientFullAccess	461
このポリシーを使用すると	461
ポリシーの詳細	461
ポリシーのバージョン	462
JSON ポリシードキュメント	462
詳細はこちら	462
AmazonElasticFileSystemClientReadOnlyAccess	462
このポリシーを使用すると	463
ポリシーの詳細	463
ポリシーのバージョン	463
JSON ポリシードキュメント	463
詳細はこちら	463
AmazonElasticFileSystemClientReadWriteAccess	464
このポリシーを使用すると	464
ポリシーの詳細	464
ポリシーのバージョン	464
JSON ポリシードキュメント	464
詳細はこちら	465

AmazonElasticFileSystemFullAccess	465
このポリシーを使用すると	465
ポリシーの詳細	465
ポリシーのバージョン	465
JSON ポリシードキュメント	466
詳細はこちら	467
AmazonElasticFileSystemReadOnlyAccess	468
このポリシーを使用すると	468
ポリシーの詳細	468
ポリシーのバージョン	468
JSON ポリシードキュメント	468
詳細はこちら	469
AmazonElasticFileSystemServiceRolePolicy	469
このポリシーを使用すると	469
ポリシーの詳細	470
ポリシーのバージョン	470
JSON ポリシードキュメント	470
詳細はこちら	472
AmazonElasticFileSystemsUtils	472
このポリシーを使用すると	472
ポリシーの詳細	472
ポリシーのバージョン	473
JSON ポリシードキュメント	473
詳細はこちら	475
AmazonElasticMapReduceEditorsRole	475
このポリシーを使用すると	475
ポリシーの詳細	475
ポリシーのバージョン	475
JSON ポリシードキュメント	476
詳細はこちら	477
AmazonElasticMapReduceforAutoScalingRole	477
このポリシーを使用すると	477
ポリシーの詳細	477
ポリシーのバージョン	477
JSON ポリシードキュメント	478
詳細はこちら	478

AmazonElasticMapReduceforEC2Role	478
このポリシーを使用すると	478
ポリシーの詳細	478
ポリシーのバージョン	479
JSON ポリシードキュメント	479
詳細はこちら	480
AmazonElasticMapReduceFullAccess	481
このポリシーを使用すると	481
ポリシーの詳細	481
ポリシーのバージョン	481
JSON ポリシードキュメント	481
詳細はこちら	483
AmazonElasticMapReducePlacementGroupPolicy	483
このポリシーを使用すると	483
ポリシーの詳細	483
ポリシーのバージョン	484
JSON ポリシードキュメント	484
詳細はこちら	484
AmazonElasticMapReduceReadOnlyAccess	485
このポリシーを使用すると	485
ポリシーの詳細	485
ポリシーのバージョン	485
JSON ポリシードキュメント	485
詳細はこちら	486
AmazonElasticMapReduceRole	486
このポリシーを使用すると	486
ポリシーの詳細	486
ポリシーのバージョン	487
JSON ポリシードキュメント	487
詳細はこちら	489
AmazonElasticsearchServiceRolePolicy	489
このポリシーを使用すると	489
ポリシーの詳細	489
ポリシーのバージョン	490
JSON ポリシードキュメント	490
詳細はこちら	493

AmazonElasticTranscoder_FullAccess	493
このポリシーを使用すると	493
ポリシーの詳細	493
ポリシーのバージョン	493
JSON ポリシードキュメント	493
詳細はこちら	494
AmazonElasticTranscoder_JobsSubmitter	494
このポリシーを使用すると	495
ポリシーの詳細	495
ポリシーのバージョン	495
JSON ポリシードキュメント	495
詳細はこちら	496
AmazonElasticTranscoder_ReadOnlyAccess	496
このポリシーを使用すると	496
ポリシーの詳細	496
ポリシーのバージョン	496
JSON ポリシードキュメント	497
詳細はこちら	497
AmazonElasticTranscoderRole	497
このポリシーを使用すると	497
ポリシーの詳細	497
ポリシーのバージョン	498
JSON ポリシードキュメント	498
詳細はこちら	499
AmazonEMRCleanupPolicy	499
このポリシーを使用すると	499
ポリシーの詳細	499
ポリシーのバージョン	499
JSON ポリシードキュメント	500
詳細はこちら	500
AmazonEMRContainersServiceRolePolicy	500
このポリシーを使用すると	501
ポリシーの詳細	501
ポリシーのバージョン	501
JSON ポリシードキュメント	501
詳細はこちら	502

AmazonEMRFullAccessPolicy_v2	502
このポリシーを使用すると	503
ポリシーの詳細	503
ポリシーのバージョン	503
JSON ポリシードキュメント	503
詳細はこちら	506
AmazonEMRReadOnlyAccessPolicy_v2	507
このポリシーを使用すると	507
ポリシーの詳細	507
ポリシーのバージョン	507
JSON ポリシードキュメント	507
詳細はこちら	508
AmazonEMRServerlessServiceRolePolicy	508
このポリシーを使用すると	509
ポリシーの詳細	509
ポリシーのバージョン	509
JSON ポリシードキュメント	509
詳細はこちら	510
AmazonEMRServicePolicy_v2	510
このポリシーを使用すると	511
ポリシーの詳細	511
ポリシーのバージョン	511
JSON ポリシードキュメント	511
詳細はこちら	519
AmazonESCognitoAccess	519
このポリシーを使用すると	519
ポリシーの詳細	519
ポリシーのバージョン	519
JSON ポリシードキュメント	519
詳細はこちら	520
AmazonESFullAccess	521
このポリシーを使用すると	521
ポリシーの詳細	521
ポリシーのバージョン	521
JSON ポリシードキュメント	521
詳細はこちら	522

AmazonESReadOnlyAccess	522
このポリシーを使用すると	522
ポリシーの詳細	522
ポリシーのバージョン	522
JSON ポリシードキュメント	522
詳細はこちら	523
AmazonEventBridgeApiDestinationsServiceRolePolicy	523
このポリシーを使用すると	523
ポリシーの詳細	523
ポリシーのバージョン	524
JSON ポリシードキュメント	524
詳細はこちら	524
AmazonEventBridgeFullAccess	524
このポリシーを使用すると	525
ポリシーの詳細	525
ポリシーのバージョン	525
JSON ポリシードキュメント	525
詳細はこちら	527
AmazonEventBridgePipesFullAccess	527
このポリシーを使用すると	528
ポリシーの詳細	528
ポリシーのバージョン	528
JSON ポリシードキュメント	528
詳細はこちら	529
AmazonEventBridgePipesOperatorAccess	529
このポリシーを使用すると	529
ポリシーの詳細	529
ポリシーのバージョン	529
JSON ポリシードキュメント	530
詳細はこちら	530
AmazonEventBridgePipesReadOnlyAccess	530
このポリシーを使用すると	531
ポリシーの詳細	531
ポリシーのバージョン	531
JSON ポリシードキュメント	531
詳細はこちら	532

AmazonEventBridgeReadOnlyAccess	532
このポリシーを使用すると	532
ポリシーの詳細	532
ポリシーのバージョン	532
JSON ポリシードキュメント	532
詳細はこちら	534
AmazonEventBridgeSchedulerFullAccess	534
このポリシーを使用すると	534
ポリシーの詳細	534
ポリシーのバージョン	534
JSON ポリシードキュメント	535
詳細はこちら	535
AmazonEventBridgeSchedulerReadOnlyAccess	535
このポリシーを使用すると	536
ポリシーの詳細	536
ポリシーのバージョン	536
JSON ポリシードキュメント	536
詳細はこちら	537
AmazonEventBridgeSchemasFullAccess	537
このポリシーを使用すると	537
ポリシーの詳細	537
ポリシーのバージョン	537
JSON ポリシードキュメント	537
詳細はこちら	538
AmazonEventBridgeSchemasReadOnlyAccess	539
このポリシーを使用すると	539
ポリシーの詳細	539
ポリシーのバージョン	539
JSON ポリシードキュメント	539
詳細はこちら	540
AmazonEventBridgeSchemasServiceRolePolicy	540
このポリシーを使用すると	540
ポリシーの詳細	540
ポリシーのバージョン	541
JSON ポリシードキュメント	541
詳細はこちら	541

AmazonFISServiceRolePolicy	542
このポリシーを使用すると	542
ポリシーの詳細	542
ポリシーのバージョン	542
JSON ポリシードキュメント	542
詳細はこちら	544
AmazonForecastFullAccess	544
このポリシーを使用すると	544
ポリシーの詳細	544
ポリシーのバージョン	544
JSON ポリシードキュメント	545
詳細はこちら	545
AmazonFraudDetectorFullAccessPolicy	546
このポリシーを使用すると	546
ポリシーの詳細	546
ポリシーのバージョン	546
JSON ポリシードキュメント	546
詳細はこちら	547
AmazonFreeRTOSFullAccess	548
このポリシーを使用すると	548
ポリシーの詳細	548
ポリシーのバージョン	548
JSON ポリシードキュメント	548
詳細はこちら	549
AmazonFreeRTOSOTAUpdate	549
このポリシーを使用すると	549
ポリシーの詳細	549
ポリシーのバージョン	549
JSON ポリシードキュメント	549
詳細はこちら	551
AmazonFSxConsoleFullAccess	551
このポリシーを使用すると	551
ポリシーの詳細	551
ポリシーのバージョン	551
JSON ポリシードキュメント	552
詳細はこちら	555

AmazonFSxConsoleReadOnlyAccess	555
このポリシーを使用すると	555
ポリシーの詳細	555
ポリシーのバージョン	556
JSON ポリシードキュメント	556
詳細はこちら	557
AmazonFSxFullAccess	557
このポリシーを使用すると	557
ポリシーの詳細	557
ポリシーのバージョン	557
JSON ポリシードキュメント	557
詳細はこちら	561
AmazonFSxReadOnlyAccess	562
このポリシーを使用すると	562
ポリシーの詳細	562
ポリシーのバージョン	562
JSON ポリシードキュメント	562
詳細はこちら	563
AmazonFSxServiceRolePolicy	563
このポリシーを使用すると	563
ポリシーの詳細	563
ポリシーのバージョン	563
JSON ポリシードキュメント	564
詳細はこちら	566
AmazonGlacierFullAccess	567
このポリシーを使用すると	567
ポリシーの詳細	567
ポリシーのバージョン	567
JSON ポリシードキュメント	567
詳細はこちら	568
AmazonGlacierReadOnlyAccess	568
このポリシーを使用すると	568
ポリシーの詳細	568
ポリシーのバージョン	568
JSON ポリシードキュメント	568
詳細はこちら	569

AmazonGrafanaAthenaAccess	569
このポリシーを使用すると	569
ポリシーの詳細	570
ポリシーのバージョン	570
JSON ポリシードキュメント	570
詳細はこちら	572
AmazonGrafanaCloudWatchAccess	572
このポリシーを使用すると	572
ポリシーの詳細	572
ポリシーのバージョン	572
JSON ポリシードキュメント	573
詳細はこちら	574
AmazonGrafanaRedshiftAccess	574
このポリシーを使用すると	574
ポリシーの詳細	574
ポリシーのバージョン	575
JSON ポリシードキュメント	575
詳細はこちら	576
AmazonGrafanaServiceLinkedRolePolicy	576
このポリシーを使用すると	576
ポリシーの詳細	576
ポリシーのバージョン	577
JSON ポリシードキュメント	577
詳細はこちら	578
AmazonGuardDutyFullAccess	578
このポリシーを使用すると	578
ポリシーの詳細	579
ポリシーのバージョン	579
JSON ポリシードキュメント	579
詳細はこちら	580
AmazonGuardDutyMalwareProtectionServiceRolePolicy	581
このポリシーを使用すると	581
ポリシーの詳細	581
ポリシーのバージョン	581
JSON ポリシードキュメント	582
詳細はこちら	586

AmazonGuardDutyReadOnlyAccess	586
このポリシーを使用すると	586
ポリシーの詳細	586
ポリシーのバージョン	587
JSON ポリシードキュメント	587
詳細はこちら	588
AmazonGuardDutyServiceRolePolicy	588
このポリシーを使用すると	588
ポリシーの詳細	588
ポリシーのバージョン	588
JSON ポリシードキュメント	589
詳細はこちら	595
AmazonHealthLakeFullAccess	595
このポリシーを使用すると	595
ポリシーの詳細	595
ポリシーのバージョン	595
JSON ポリシードキュメント	595
詳細はこちら	596
AmazonHealthLakeReadOnlyAccess	596
このポリシーを使用すると	596
ポリシーの詳細	597
ポリシーのバージョン	597
JSON ポリシードキュメント	597
詳細はこちら	597
AmazonHoneycodeFullAccess	598
このポリシーを使用すると	598
ポリシーの詳細	598
ポリシーのバージョン	598
JSON ポリシードキュメント	598
詳細はこちら	599
AmazonHoneycodeReadOnlyAccess	599
このポリシーを使用すると	599
ポリシーの詳細	599
ポリシーのバージョン	599
JSON ポリシードキュメント	600
詳細はこちら	600

AmazonHoneycodeServiceRolePolicy	600
このポリシーを使用すると	601
ポリシーの詳細	601
ポリシーのバージョン	601
JSON ポリシードキュメント	601
詳細はこちら	602
AmazonHoneycodeTeamAssociationFullAccess	602
このポリシーを使用すると	602
ポリシーの詳細	602
ポリシーのバージョン	602
JSON ポリシードキュメント	602
詳細はこちら	603
AmazonHoneycodeTeamAssociationReadOnlyAccess	603
このポリシーを使用すると	603
ポリシーの詳細	603
ポリシーのバージョン	604
JSON ポリシードキュメント	604
詳細はこちら	604
AmazonHoneycodeWorkbookFullAccess	604
このポリシーを使用すると	605
ポリシーの詳細	605
ポリシーのバージョン	605
JSON ポリシードキュメント	605
詳細はこちら	606
AmazonHoneycodeWorkbookReadOnlyAccess	606
このポリシーを使用すると	606
ポリシーの詳細	606
ポリシーのバージョン	606
JSON ポリシードキュメント	607
詳細はこちら	607
AmazonInspector2AgentlessServiceRolePolicy	607
このポリシーを使用すると	608
ポリシーの詳細	608
ポリシーのバージョン	608
JSON ポリシードキュメント	608
詳細はこちら	612

AmazonInspector2FullAccess	612
このポリシーを使用すると	612
ポリシーの詳細	612
ポリシーのバージョン	612
JSON ポリシードキュメント	613
詳細はこちら	614
AmazonInspector2ManagedCisPolicy	614
このポリシーを使用すると	614
ポリシーの詳細	614
ポリシーのバージョン	614
JSON ポリシードキュメント	615
詳細はこちら	615
AmazonInspector2ReadOnlyAccess	615
このポリシーを使用すると	616
ポリシーの詳細	616
ポリシーのバージョン	616
JSON ポリシードキュメント	616
詳細はこちら	617
AmazonInspector2ServiceRolePolicy	617
このポリシーを使用すると	617
ポリシーの詳細	617
ポリシーのバージョン	617
JSON ポリシードキュメント	618
詳細はこちら	624
AmazonInspectorFullAccess	624
このポリシーを使用すると	624
ポリシーの詳細	624
ポリシーのバージョン	625
JSON ポリシードキュメント	625
詳細はこちら	626
AmazonInspectorReadOnlyAccess	626
このポリシーを使用すると	626
ポリシーの詳細	626
ポリシーのバージョン	626
JSON ポリシードキュメント	627
詳細はこちら	627

AmazonInspectorServiceRolePolicy	627
このポリシーを使用すると	628
ポリシーの詳細	628
ポリシーのバージョン	628
JSON ポリシードキュメント	628
詳細はこちら	629
AmazonKendraFullAccess	630
このポリシーを使用すると	630
ポリシーの詳細	630
ポリシーのバージョン	630
JSON ポリシードキュメント	630
詳細はこちら	632
AmazonKendraReadOnlyAccess	632
このポリシーを使用すると	632
ポリシーの詳細	632
ポリシーのバージョン	633
JSON ポリシードキュメント	633
詳細はこちら	633
AmazonKeyspacesFullAccess	634
このポリシーを使用すると	634
ポリシーの詳細	634
ポリシーのバージョン	634
JSON ポリシードキュメント	634
詳細はこちら	636
AmazonKeyspacesReadOnlyAccess	636
このポリシーを使用すると	636
ポリシーの詳細	636
ポリシーのバージョン	637
JSON ポリシードキュメント	637
詳細はこちら	638
AmazonKeyspacesReadOnlyAccess_v2	638
このポリシーを使用すると	638
ポリシーの詳細	638
ポリシーのバージョン	638
JSON ポリシードキュメント	638
詳細はこちら	639

AmazonKinesisAnalyticsFullAccess	640
このポリシーを使用すると	640
ポリシーの詳細	640
ポリシーのバージョン	640
JSON ポリシードキュメント	640
詳細はこちら	642
AmazonKinesisAnalyticsReadOnly	642
このポリシーを使用すると	642
ポリシーの詳細	642
ポリシーのバージョン	642
JSON ポリシードキュメント	643
詳細はこちら	644
AmazonKinesisFirehoseFullAccess	644
このポリシーを使用すると	644
ポリシーの詳細	644
ポリシーのバージョン	645
JSON ポリシードキュメント	645
詳細はこちら	645
AmazonKinesisFirehoseReadOnlyAccess	645
このポリシーを使用すると	646
ポリシーの詳細	646
ポリシーのバージョン	646
JSON ポリシードキュメント	646
詳細はこちら	646
AmazonKinesisFullAccess	647
このポリシーを使用すると	647
ポリシーの詳細	647
ポリシーのバージョン	647
JSON ポリシードキュメント	647
詳細はこちら	648
AmazonKinesisReadOnlyAccess	648
このポリシーを使用すると	648
ポリシーの詳細	648
ポリシーのバージョン	648
JSON ポリシードキュメント	649
詳細はこちら	649

AmazonKinesisVideoStreamsFullAccess	649
このポリシーを使用すると	649
ポリシーの詳細	649
ポリシーのバージョン	650
JSON ポリシードキュメント	650
詳細はこちら	650
AmazonKinesisVideoStreamsReadOnlyAccess	650
このポリシーを使用すると	651
ポリシーの詳細	651
ポリシーのバージョン	651
JSON ポリシードキュメント	651
詳細はこちら	652
AmazonLaunchWizard_Fullaccess	652
このポリシーを使用すると	652
ポリシーの詳細	652
ポリシーのバージョン	652
JSON ポリシードキュメント	652
詳細はこちら	667
AmazonLaunchWizardFullAccessV2	667
このポリシーを使用すると	667
ポリシーの詳細	667
ポリシーのバージョン	667
JSON ポリシードキュメント	667
詳細はこちら	684
AmazonLexChannelsAccess	684
このポリシーを使用すると	684
ポリシーの詳細	684
ポリシーのバージョン	685
JSON ポリシードキュメント	685
詳細はこちら	685
AmazonLexFullAccess	685
このポリシーを使用すると	685
ポリシーの詳細	686
ポリシーのバージョン	686
JSON ポリシードキュメント	686
詳細はこちら	691

AmazonLexReadOnly	692
このポリシーを使用すると	692
ポリシーの詳細	692
ポリシーのバージョン	692
JSON ポリシードキュメント	692
詳細はこちら	694
AmazonLexReplicationPolicy	694
このポリシーを使用すると	694
ポリシーの詳細	694
ポリシーのバージョン	695
JSON ポリシードキュメント	695
詳細はこちら	697
AmazonLexRunBotsOnly	697
このポリシーを使用すると	697
ポリシーの詳細	697
ポリシーのバージョン	697
JSON ポリシードキュメント	698
詳細はこちら	698
AmazonLexV2BotPolicy	698
このポリシーを使用すると	699
ポリシーの詳細	699
ポリシーのバージョン	699
JSON ポリシードキュメント	699
詳細はこちら	700
AmazonLookoutEquipmentFullAccess	700
このポリシーを使用すると	700
ポリシーの詳細	700
ポリシーのバージョン	700
JSON ポリシードキュメント	700
詳細はこちら	702
AmazonLookoutEquipmentReadOnlyAccess	702
このポリシーを使用すると	702
ポリシーの詳細	702
ポリシーのバージョン	702
JSON ポリシードキュメント	702
詳細はこちら	703

AmazonLookoutMetricsFullAccess	703
このポリシーを使用すると	703
ポリシーの詳細	703
ポリシーのバージョン	704
JSON ポリシードキュメント	704
詳細はこちら	704
AmazonLookoutMetricsReadOnlyAccess	705
このポリシーを使用すると	705
ポリシーの詳細	705
ポリシーのバージョン	705
JSON ポリシードキュメント	705
詳細はこちら	706
AmazonLookoutVisionConsoleFullAccess	706
このポリシーを使用すると	706
ポリシーの詳細	706
ポリシーのバージョン	707
JSON ポリシードキュメント	707
詳細はこちら	709
AmazonLookoutVisionConsoleReadOnlyAccess	709
このポリシーを使用すると	709
ポリシーの詳細	709
ポリシーのバージョン	710
JSON ポリシードキュメント	710
詳細はこちら	711
AmazonLookoutVisionFullAccess	711
このポリシーを使用すると	711
ポリシーの詳細	712
ポリシーのバージョン	712
JSON ポリシードキュメント	712
詳細はこちら	712
AmazonLookoutVisionReadOnlyAccess	713
このポリシーを使用すると	713
ポリシーの詳細	713
ポリシーのバージョン	713
JSON ポリシードキュメント	713
詳細はこちら	714

AmazonMachineLearningBatchPredictionsAccess	714
このポリシーを使用すると	714
ポリシーの詳細	714
ポリシーのバージョン	715
JSON ポリシードキュメント	715
詳細はこちら	715
AmazonMachineLearningCreateOnlyAccess	715
このポリシーを使用すると	716
ポリシーの詳細	716
ポリシーのバージョン	716
JSON ポリシードキュメント	716
詳細はこちら	717
AmazonMachineLearningFullAccess	717
このポリシーを使用すると	717
ポリシーの詳細	717
ポリシーのバージョン	717
JSON ポリシードキュメント	717
詳細はこちら	718
AmazonMachineLearningManageRealTimeEndpointOnlyAccess	718
このポリシーを使用すると	718
ポリシーの詳細	718
ポリシーのバージョン	719
JSON ポリシードキュメント	719
詳細はこちら	719
AmazonMachineLearningReadOnlyAccess	719
このポリシーを使用すると	720
ポリシーの詳細	720
ポリシーのバージョン	720
JSON ポリシードキュメント	720
詳細はこちら	720
AmazonMachineLearningRealTimePredictionOnlyAccess	721
このポリシーを使用すると	721
ポリシーの詳細	721
ポリシーのバージョン	721
JSON ポリシードキュメント	721
詳細はこちら	722

AmazonMachineLearningRoleforRedshiftDataSourceV3	722
このポリシーを使用すると	722
ポリシーの詳細	722
ポリシーのバージョン	723
JSON ポリシードキュメント	723
詳細はこちら	724
AmazonMacieFullAccess	724
このポリシーを使用すると	724
ポリシーの詳細	724
ポリシーのバージョン	724
JSON ポリシードキュメント	725
詳細はこちら	725
AmazonMacieHandshakeRole	726
このポリシーを使用すると	726
ポリシーの詳細	726
ポリシーのバージョン	726
JSON ポリシードキュメント	726
詳細はこちら	727
AmazonMacieReadOnlyAccess	727
このポリシーを使用すると	727
ポリシーの詳細	727
ポリシーのバージョン	727
JSON ポリシードキュメント	728
詳細はこちら	728
AmazonMacieServiceRole	728
このポリシーを使用すると	728
ポリシーの詳細	729
ポリシーのバージョン	729
JSON ポリシードキュメント	729
詳細はこちら	729
AmazonMacieServiceRolePolicy	730
このポリシーを使用すると	730
ポリシーの詳細	730
ポリシーのバージョン	730
JSON ポリシードキュメント	730
詳細はこちら	732

AmazonManagedBlockchainConsoleFullAccess	732
このポリシーを使用すると	732
ポリシーの詳細	732
ポリシーのバージョン	732
JSON ポリシードキュメント	732
詳細はこちら	733
AmazonManagedBlockchainFullAccess	733
このポリシーを使用すると	733
ポリシーの詳細	733
ポリシーのバージョン	734
JSON ポリシードキュメント	734
詳細はこちら	734
AmazonManagedBlockchainReadOnlyAccess	734
このポリシーを使用すると	735
ポリシーの詳細	735
ポリシーのバージョン	735
JSON ポリシードキュメント	735
詳細はこちら	736
AmazonManagedBlockchainServiceRolePolicy	736
このポリシーを使用すると	736
ポリシーの詳細	736
ポリシーのバージョン	736
JSON ポリシードキュメント	737
詳細はこちら	737
AmazonMCSFullAccess	737
このポリシーを使用すると	737
ポリシーの詳細	738
ポリシーのバージョン	738
JSON ポリシードキュメント	738
詳細はこちら	739
AmazonMCSReadOnlyAccess	739
このポリシーを使用すると	740
ポリシーの詳細	740
ポリシーのバージョン	740
JSON ポリシードキュメント	740
詳細はこちら	741

AmazonMechanicalTurkFullAccess	741
このポリシーを使用すると	741
ポリシーの詳細	741
ポリシーのバージョン	741
JSON ポリシードキュメント	742
詳細はこちら	742
AmazonMechanicalTurkReadOnly	742
このポリシーを使用すると	742
ポリシーの詳細	742
ポリシーのバージョン	743
JSON ポリシードキュメント	743
詳細はこちら	743
AmazonMemoryDBFullAccess	743
このポリシーを使用すると	744
ポリシーの詳細	744
ポリシーのバージョン	744
JSON ポリシードキュメント	744
詳細はこちら	745
AmazonMemoryDBReadOnlyAccess	745
このポリシーを使用すると	745
ポリシーの詳細	745
ポリシーのバージョン	745
JSON ポリシードキュメント	746
詳細はこちら	746
AmazonMobileAnalyticsFinancialReportAccess	746
このポリシーを使用すると	746
ポリシーの詳細	746
ポリシーのバージョン	747
JSON ポリシードキュメント	747
詳細はこちら	747
AmazonMobileAnalyticsFullAccess	747
このポリシーを使用すると	748
ポリシーの詳細	748
ポリシーのバージョン	748
JSON ポリシードキュメント	748
詳細はこちら	748

AmazonMobileAnalyticsNon-financialReportAccess	749
このポリシーを使用すると	749
ポリシーの詳細	749
ポリシーのバージョン	749
JSON ポリシードキュメント	749
詳細はこちら	750
AmazonMobileAnalyticsWriteOnlyAccess	750
このポリシーを使用すると	750
ポリシーの詳細	750
ポリシーのバージョン	750
JSON ポリシードキュメント	751
詳細はこちら	751
AmazonMonitronFullAccess	751
このポリシーを使用すると	751
ポリシーの詳細	751
ポリシーのバージョン	752
JSON ポリシードキュメント	752
詳細はこちら	754
AmazonMQApiFullAccess	754
このポリシーを使用すると	754
ポリシーの詳細	754
ポリシーのバージョン	754
JSON ポリシードキュメント	754
詳細はこちら	756
AmazonMQApiReadOnlyAccess	756
このポリシーを使用すると	756
ポリシーの詳細	756
ポリシーのバージョン	756
JSON ポリシードキュメント	756
詳細はこちら	757
AmazonMQFullAccess	757
このポリシーを使用すると	757
ポリシーの詳細	757
ポリシーのバージョン	758
JSON ポリシードキュメント	758
詳細はこちら	759

AmazonMQReadOnlyAccess	759
このポリシーを使用すると	759
ポリシーの詳細	759
ポリシーのバージョン	760
JSON ポリシードキュメント	760
詳細はこちら	760
AmazonMQServiceRolePolicy	760
このポリシーを使用すると	761
ポリシーの詳細	761
ポリシーのバージョン	761
JSON ポリシードキュメント	761
詳細はこちら	763
AmazonMSKConnectReadOnlyAccess	763
このポリシーを使用すると	763
ポリシーの詳細	763
ポリシーのバージョン	763
JSON ポリシードキュメント	764
詳細はこちら	765
AmazonMSKFullAccess	765
このポリシーを使用すると	765
ポリシーの詳細	765
ポリシーのバージョン	765
JSON ポリシードキュメント	766
詳細はこちら	768
AmazonMSKReadOnlyAccess	769
このポリシーを使用すると	769
ポリシーの詳細	769
ポリシーのバージョン	769
JSON ポリシードキュメント	769
詳細はこちら	770
AmazonMWAAServiceRolePolicy	770
このポリシーを使用すると	770
ポリシーの詳細	770
ポリシーのバージョン	770
JSON ポリシードキュメント	771
詳細はこちら	773

AmazonNimbleStudio-LaunchProfileWorker	773
このポリシーを使用すると	773
ポリシーの詳細	773
ポリシーのバージョン	774
JSON ポリシードキュメント	774
詳細はこちら	774
AmazonNimbleStudio-StudioAdmin	775
このポリシーを使用すると	775
ポリシーの詳細	775
ポリシーのバージョン	775
JSON ポリシードキュメント	775
詳細はこちら	777
AmazonNimbleStudio-StudioUser	777
このポリシーを使用すると	777
ポリシーの詳細	778
ポリシーのバージョン	778
JSON ポリシードキュメント	778
詳細はこちら	780
AmazonOmicsFullAccess	780
このポリシーを使用すると	780
ポリシーの詳細	780
ポリシーのバージョン	781
JSON ポリシードキュメント	781
詳細はこちら	782
AmazonOmicsReadOnlyAccess	782
このポリシーを使用すると	782
ポリシーの詳細	782
ポリシーのバージョン	782
JSON ポリシードキュメント	783
詳細はこちら	783
AmazonOneEnterpriseFullAccess	783
このポリシーを使用すると	783
ポリシーの詳細	784
ポリシーのバージョン	784
JSON ポリシードキュメント	784
詳細はこちら	784

AmazonOneEnterpriseInstallerAccess	785
このポリシーを使用すると	785
ポリシーの詳細	785
ポリシーのバージョン	785
JSON ポリシードキュメント	785
詳細はこちら	786
AmazonOneEnterpriseReadOnlyAccess	786
このポリシーを使用すると	786
ポリシーの詳細	786
ポリシーのバージョン	786
JSON ポリシードキュメント	787
詳細はこちら	787
AmazonOpenSearchDashboardsServiceRolePolicy	787
このポリシーを使用すると	788
ポリシーの詳細	788
ポリシーのバージョン	788
JSON ポリシードキュメント	788
詳細はこちら	789
AmazonOpenSearchDirectQueryGlueCreateAccess	789
このポリシーを使用すると	789
ポリシーの詳細	789
ポリシーのバージョン	789
JSON ポリシードキュメント	789
詳細はこちら	790
AmazonOpenSearchIngestionFullAccess	790
このポリシーを使用すると	790
ポリシーの詳細	790
ポリシーのバージョン	791
JSON ポリシードキュメント	791
詳細はこちら	792
AmazonOpenSearchIngestionReadOnlyAccess	792
このポリシーを使用すると	792
ポリシーの詳細	792
ポリシーのバージョン	792
JSON ポリシードキュメント	793
詳細はこちら	793

AmazonOpenSearchIngestionServiceRolePolicy	793
このポリシーを使用すると	794
ポリシーの詳細	794
ポリシーのバージョン	794
JSON ポリシードキュメント	794
詳細はこちら	796
AmazonOpenSearchServerlessServiceRolePolicy	796
このポリシーを使用すると	796
ポリシーの詳細	796
ポリシーのバージョン	797
JSON ポリシードキュメント	797
詳細はこちら	797
AmazonOpenSearchServiceCognitoAccess	797
このポリシーを使用すると	798
ポリシーの詳細	798
ポリシーのバージョン	798
JSON ポリシードキュメント	798
詳細はこちら	799
AmazonOpenSearchServiceFullAccess	799
このポリシーを使用すると	800
ポリシーの詳細	800
ポリシーのバージョン	800
JSON ポリシードキュメント	800
詳細はこちら	800
AmazonOpenSearchServiceReadOnlyAccess	801
このポリシーを使用すると	801
ポリシーの詳細	801
ポリシーのバージョン	801
JSON ポリシードキュメント	801
詳細はこちら	802
AmazonOpenSearchServiceRolePolicy	802
このポリシーを使用すると	802
ポリシーの詳細	802
ポリシーのバージョン	803
JSON ポリシードキュメント	803
詳細はこちら	807

AmazonPersonalizeFullAccess	807
このポリシーを使用すると	808
ポリシーの詳細	808
ポリシーのバージョン	808
JSON ポリシードキュメント	808
詳細はこちら	809
AmazonPollyFullAccess	809
このポリシーを使用すると	810
ポリシーの詳細	810
ポリシーのバージョン	810
JSON ポリシードキュメント	810
詳細はこちら	810
AmazonPollyReadOnlyAccess	811
このポリシーを使用すると	811
ポリシーの詳細	811
ポリシーのバージョン	811
JSON ポリシードキュメント	811
詳細はこちら	812
AmazonPrometheusConsoleFullAccess	812
このポリシーを使用すると	812
ポリシーの詳細	812
ポリシーのバージョン	813
JSON ポリシードキュメント	813
詳細はこちら	814
AmazonPrometheusFullAccess	814
このポリシーを使用すると	814
ポリシーの詳細	814
ポリシーのバージョン	814
JSON ポリシードキュメント	815
詳細はこちら	816
AmazonPrometheusQueryAccess	816
このポリシーを使用すると	816
ポリシーの詳細	816
ポリシーのバージョン	816
JSON ポリシードキュメント	817
詳細はこちら	817

AmazonPrometheusRemoteWriteAccess	817
このポリシーを使用すると	817
ポリシーの詳細	817
ポリシーのバージョン	818
JSON ポリシードキュメント	818
詳細はこちら	818
AmazonPrometheusScraperServiceRolePolicy	818
このポリシーを使用すると	819
ポリシーの詳細	819
ポリシーのバージョン	819
JSON ポリシードキュメント	819
詳細はこちら	821
AmazonQFullAccess	822
このポリシーを使用すると	822
ポリシーの詳細	822
ポリシーのバージョン	822
JSON ポリシードキュメント	822
詳細はこちら	823
AmazonQLDBConsoleFullAccess	823
このポリシーを使用すると	823
ポリシーの詳細	823
ポリシーのバージョン	824
JSON ポリシードキュメント	824
詳細はこちら	825
AmazonQLDBFullAccess	826
このポリシーを使用すると	826
ポリシーの詳細	826
ポリシーのバージョン	826
JSON ポリシードキュメント	826
詳細はこちら	828
AmazonQLDBReadOnly	828
このポリシーを使用すると	828
ポリシーの詳細	828
ポリシーのバージョン	828
JSON ポリシードキュメント	828
詳細はこちら	829

AmazonRDSBetaServiceRolePolicy	829
このポリシーを使用すると	829
ポリシーの詳細	830
ポリシーのバージョン	830
JSON ポリシードキュメント	830
詳細はこちら	833
AmazonRDSCustomInstanceProfileRolePolicy	833
このポリシーを使用すると	833
ポリシーの詳細	834
ポリシーのバージョン	834
JSON ポリシードキュメント	834
詳細はこちら	841
AmazonRDSCustomPreviewServiceRolePolicy	841
このポリシーを使用すると	842
ポリシーの詳細	842
ポリシーのバージョン	842
JSON ポリシードキュメント	842
詳細はこちら	858
AmazonRDSCustomServiceRolePolicy	858
このポリシーを使用すると	858
ポリシーの詳細	858
ポリシーのバージョン	858
JSON ポリシードキュメント	859
詳細はこちら	876
AmazonRDSDataFullAccess	876
このポリシーを使用すると	876
ポリシーの詳細	876
ポリシーのバージョン	876
JSON ポリシードキュメント	877
詳細はこちら	878
AmazonRDSDirectoryServiceAccess	878
このポリシーを使用すると	878
ポリシーの詳細	878
ポリシーのバージョン	878
JSON ポリシードキュメント	879
詳細はこちら	879

AmazonRDSEnhancedMonitoringRole	879
このポリシーを使用すると	879
ポリシーの詳細	880
ポリシーのバージョン	880
JSON ポリシードキュメント	880
詳細はこちら	881
AmazonRDSFullAccess	881
このポリシーを使用すると	881
ポリシーの詳細	881
ポリシーのバージョン	881
JSON ポリシードキュメント	882
詳細はこちら	884
AmazonRDSPerformanceInsightsFullAccess	884
このポリシーを使用すると	884
ポリシーの詳細	884
ポリシーのバージョン	884
JSON ポリシードキュメント	884
詳細はこちら	886
AmazonRDSPerformanceInsightsReadOnly	886
このポリシーを使用すると	886
ポリシーの詳細	886
ポリシーのバージョン	887
JSON ポリシードキュメント	887
詳細はこちら	888
AmazonRDSPreviewServiceRolePolicy	889
このポリシーを使用すると	889
ポリシーの詳細	889
ポリシーのバージョン	889
JSON ポリシードキュメント	889
詳細はこちら	893
AmazonRDSReadOnlyAccess	893
このポリシーを使用すると	893
ポリシーの詳細	893
ポリシーのバージョン	893
JSON ポリシードキュメント	893
詳細はこちら	895

AmazonRDSServiceRolePolicy	895
このポリシーを使用すると	895
ポリシーの詳細	895
ポリシーのバージョン	895
JSON ポリシードキュメント	896
詳細はこちら	899
AmazonRedshiftAllCommandsFullAccess	900
このポリシーを使用すると	900
ポリシーの詳細	900
ポリシーのバージョン	900
JSON ポリシードキュメント	900
詳細はこちら	906
AmazonRedshiftDataFullAccess	906
このポリシーを使用すると	906
ポリシーの詳細	906
ポリシーのバージョン	906
JSON ポリシードキュメント	906
詳細はこちら	908
AmazonRedshiftFullAccess	909
このポリシーを使用すると	909
ポリシーの詳細	909
ポリシーのバージョン	909
JSON ポリシードキュメント	909
詳細はこちら	911
AmazonRedshiftQueryEditor	911
このポリシーを使用すると	912
ポリシーの詳細	912
ポリシーのバージョン	912
JSON ポリシードキュメント	912
詳細はこちら	914
AmazonRedshiftQueryEditorV2FullAccess	914
このポリシーを使用すると	914
ポリシーの詳細	915
ポリシーのバージョン	915
JSON ポリシードキュメント	915
詳細はこちら	916

AmazonRedshiftQueryEditorV2NoSharing	917
このポリシーを使用すると	917
ポリシーの詳細	917
ポリシーのバージョン	917
JSON ポリシードキュメント	917
詳細はこちら	921
AmazonRedshiftQueryEditorV2ReadSharing	921
このポリシーを使用すると	921
ポリシーの詳細	922
ポリシーのバージョン	922
JSON ポリシードキュメント	922
詳細はこちら	927
AmazonRedshiftQueryEditorV2ReadWriteSharing	927
このポリシーを使用すると	927
ポリシーの詳細	927
ポリシーのバージョン	928
JSON ポリシードキュメント	928
詳細はこちら	933
AmazonRedshiftReadOnlyAccess	933
このポリシーを使用すると	933
ポリシーの詳細	933
ポリシーのバージョン	933
JSON ポリシードキュメント	934
詳細はこちら	934
AmazonRedshiftServiceLinkedRolePolicy	935
このポリシーを使用すると	935
ポリシーの詳細	935
ポリシーのバージョン	935
JSON ポリシードキュメント	935
詳細はこちら	941
AmazonRekognitionCustomLabelsFullAccess	941
このポリシーを使用すると	941
ポリシーの詳細	941
ポリシーのバージョン	941
JSON ポリシードキュメント	941
詳細はこちら	943

AmazonRekognitionFullAccess	943
このポリシーを使用すると	943
ポリシーの詳細	943
ポリシーのバージョン	943
JSON ポリシードキュメント	944
詳細はこちら	944
AmazonRekognitionReadOnlyAccess	944
このポリシーを使用すると	944
ポリシーの詳細	944
ポリシーのバージョン	945
JSON ポリシードキュメント	945
詳細はこちら	946
AmazonRekognitionServiceRole	946
このポリシーを使用すると	946
ポリシーの詳細	946
ポリシーのバージョン	947
JSON ポリシードキュメント	947
詳細はこちら	948
AmazonRoute53AutoNamingFullAccess	948
このポリシーを使用すると	948
ポリシーの詳細	948
ポリシーのバージョン	948
JSON ポリシードキュメント	948
詳細はこちら	949
AmazonRoute53AutoNamingReadOnlyAccess	949
このポリシーを使用すると	950
ポリシーの詳細	950
ポリシーのバージョン	950
JSON ポリシードキュメント	950
詳細はこちら	951
AmazonRoute53AutoNamingRegistrantAccess	951
このポリシーを使用すると	951
ポリシーの詳細	951
ポリシーのバージョン	951
JSON ポリシードキュメント	951
詳細はこちら	952

AmazonRoute53DomainsFullAccess	952
このポリシーを使用すると	952
ポリシーの詳細	953
ポリシーのバージョン	953
JSON ポリシードキュメント	953
詳細はこちら	953
AmazonRoute53DomainsReadOnlyAccess	954
このポリシーを使用すると	954
ポリシーの詳細	954
ポリシーのバージョン	954
JSON ポリシードキュメント	954
詳細はこちら	955
AmazonRoute53FullAccess	955
このポリシーを使用すると	955
ポリシーの詳細	955
ポリシーのバージョン	955
JSON ポリシードキュメント	956
詳細はこちら	956
AmazonRoute53ProfilesFullAccess	957
このポリシーを使用すると	957
ポリシーの詳細	957
ポリシーのバージョン	957
JSON ポリシードキュメント	957
詳細はこちら	958
AmazonRoute53ProfilesReadOnlyAccess	959
このポリシーを使用すると	959
ポリシーの詳細	959
ポリシーのバージョン	959
JSON ポリシードキュメント	959
詳細はこちら	960
AmazonRoute53ReadOnlyAccess	960
このポリシーを使用すると	960
ポリシーの詳細	960
ポリシーのバージョン	961
JSON ポリシードキュメント	961
詳細はこちら	961

AmazonRoute53RecoveryClusterFullAccess	961
このポリシーを使用すると	962
ポリシーの詳細	962
ポリシーのバージョン	962
JSON ポリシードキュメント	962
詳細はこちら	962
AmazonRoute53RecoveryClusterReadOnlyAccess	963
このポリシーを使用すると	963
ポリシーの詳細	963
ポリシーのバージョン	963
JSON ポリシードキュメント	963
詳細はこちら	964
AmazonRoute53RecoveryControlConfigFullAccess	964
このポリシーを使用すると	964
ポリシーの詳細	964
ポリシーのバージョン	964
JSON ポリシードキュメント	965
詳細はこちら	965
AmazonRoute53RecoveryControlConfigReadOnlyAccess	965
このポリシーを使用すると	965
ポリシーの詳細	965
ポリシーのバージョン	966
JSON ポリシードキュメント	966
詳細はこちら	966
AmazonRoute53RecoveryReadinessFullAccess	967
このポリシーを使用すると	967
ポリシーの詳細	967
ポリシーのバージョン	967
JSON ポリシードキュメント	967
詳細はこちら	968
AmazonRoute53RecoveryReadinessReadOnlyAccess	968
このポリシーを使用すると	968
ポリシーの詳細	968
ポリシーのバージョン	968
JSON ポリシードキュメント	969
詳細はこちら	970

AmazonRoute53ResolverFullAccess	970
このポリシーを使用すると	970
ポリシーの詳細	970
ポリシーのバージョン	970
JSON ポリシードキュメント	970
詳細はこちら	971
AmazonRoute53ResolverReadOnlyAccess	971
このポリシーを使用すると	971
ポリシーの詳細	972
ポリシーのバージョン	972
JSON ポリシードキュメント	972
詳細はこちら	972
AmazonS3FullAccess	973
このポリシーを使用すると	973
ポリシーの詳細	973
ポリシーのバージョン	973
JSON ポリシードキュメント	973
詳細はこちら	974
AmazonS3ObjectLambdaExecutionRolePolicy	974
このポリシーを使用すると	974
ポリシーの詳細	974
ポリシーのバージョン	974
JSON ポリシードキュメント	975
詳細はこちら	975
AmazonS3OutpostsFullAccess	975
このポリシーを使用すると	975
ポリシーの詳細	976
ポリシーのバージョン	976
JSON ポリシードキュメント	976
詳細はこちら	977
AmazonS3OutpostsReadOnlyAccess	977
このポリシーを使用すると	977
ポリシーの詳細	977
ポリシーのバージョン	978
JSON ポリシードキュメント	978
詳細はこちら	979

AmazonS3ReadOnlyAccess	979
このポリシーを使用すると	979
ポリシーの詳細	979
ポリシーのバージョン	980
JSON ポリシードキュメント	980
詳細はこちら	980
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy	981
このポリシーを使用すると	981
ポリシーの詳細	981
ポリシーのバージョン	981
JSON ポリシードキュメント	981
詳細はこちら	991
AmazonSageMakerCanvasAIServicesAccess	992
このポリシーを使用すると	992
ポリシーの詳細	992
ポリシーのバージョン	992
JSON ポリシードキュメント	992
詳細はこちら	995
AmazonSageMakerCanvasBedrockAccess	996
このポリシーを使用すると	996
ポリシーの詳細	996
ポリシーのバージョン	996
JSON ポリシードキュメント	996
詳細はこちら	997
AmazonSageMakerCanvasDataPrepFullAccess	997
このポリシーを使用すると	997
ポリシーの詳細	998
ポリシーのバージョン	998
JSON ポリシードキュメント	998
詳細はこちら	1005
AmazonSageMakerCanvasDirectDeployAccess	1005
このポリシーを使用すると	1005
ポリシーの詳細	1005
ポリシーのバージョン	1006
JSON ポリシードキュメント	1006
詳細はこちら	1007

AmazonSageMakerCanvasForecastAccess	1007
このポリシーを使用すると	1007
ポリシーの詳細	1007
ポリシーのバージョン	1007
JSON ポリシードキュメント	1008
詳細はこちら	1008
AmazonSageMakerCanvasFullAccess	1008
このポリシーを使用すると	1009
ポリシーの詳細	1009
ポリシーのバージョン	1009
JSON ポリシードキュメント	1009
詳細はこちら	1017
AmazonSageMakerClusterInstanceRolePolicy	1017
このポリシーを使用すると	1017
ポリシーの詳細	1018
ポリシーのバージョン	1018
JSON ポリシードキュメント	1018
詳細はこちら	1020
AmazonSageMakerCoreServiceRolePolicy	1020
このポリシーを使用すると	1020
ポリシーの詳細	1020
ポリシーのバージョン	1020
JSON ポリシードキュメント	1021
詳細はこちら	1022
AmazonSageMakerEdgeDeviceFleetPolicy	1022
このポリシーを使用すると	1022
ポリシーの詳細	1022
ポリシーのバージョン	1022
JSON ポリシードキュメント	1022
詳細はこちら	1024
AmazonSageMakerFeatureStoreAccess	1024
このポリシーを使用すると	1025
ポリシーの詳細	1025
ポリシーのバージョン	1025
JSON ポリシードキュメント	1025
詳細はこちら	1026

AmazonSageMakerFullAccess	1026
このポリシーを使用すると	1027
ポリシーの詳細	1027
ポリシーのバージョン	1027
JSON ポリシードキュメント	1027
詳細はこちら	1043
AmazonSageMakerGeospatialExecutionRole	1043
このポリシーを使用すると	1043
ポリシーの詳細	1044
ポリシーのバージョン	1044
JSON ポリシードキュメント	1044
詳細はこちら	1045
AmazonSageMakerGeospatialFullAccess	1045
このポリシーを使用すると	1045
ポリシーの詳細	1045
ポリシーのバージョン	1046
JSON ポリシードキュメント	1046
詳細はこちら	1046
AmazonSageMakerGroundTruthExecution	1047
このポリシーを使用すると	1047
ポリシーの詳細	1047
ポリシーのバージョン	1047
JSON ポリシードキュメント	1047
詳細はこちら	1051
AmazonSageMakerMechanicalTurkAccess	1051
このポリシーを使用すると	1051
ポリシーの詳細	1051
ポリシーのバージョン	1051
JSON ポリシードキュメント	1052
詳細はこちら	1052
AmazonSageMakerModelGovernanceUseAccess	1052
このポリシーを使用すると	1052
ポリシーの詳細	1053
ポリシーのバージョン	1053
JSON ポリシードキュメント	1053
詳細はこちら	1055

AmazonSageMakerModelRegistryFullAccess	1055
このポリシーを使用すると	1055
ポリシーの詳細	1055
ポリシーのバージョン	1056
JSON ポリシードキュメント	1056
詳細はこちら	1059
AmazonSageMakerNotebooksServiceRolePolicy	1060
このポリシーを使用すると	1060
ポリシーの詳細	1060
ポリシーのバージョン	1060
JSON ポリシードキュメント	1060
詳細はこちら	1064
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy	1064
このポリシーを使用すると	1065
ポリシーの詳細	1065
ポリシーのバージョン	1065
JSON ポリシードキュメント	1065
詳細はこちら	1066
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy	1066
このポリシーを使用すると	1066
ポリシーの詳細	1067
ポリシーのバージョン	1067
JSON ポリシードキュメント	1067
詳細はこちら	1070
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy	1071
このポリシーを使用すると	1071
ポリシーの詳細	1071
ポリシーのバージョン	1071
JSON ポリシードキュメント	1071
詳細はこちら	1072
AmazonSageMakerPipelinesIntegrations	1072
このポリシーを使用すると	1072
ポリシーの詳細	1072
ポリシーのバージョン	1073
JSON ポリシードキュメント	1073
詳細はこちら	1075

AmazonSageMakerReadOnly	1075
このポリシーを使用すると	1075
ポリシーの詳細	1075
ポリシーのバージョン	1075
JSON ポリシードキュメント	1076
詳細はこちら	1077
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy	1077
このポリシーを使用すると	1077
ポリシーの詳細	1077
ポリシーのバージョン	1078
JSON ポリシードキュメント	1078
詳細はこちら	1079
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy	1079
このポリシーを使用すると	1079
ポリシーの詳細	1079
ポリシーのバージョン	1079
JSON ポリシードキュメント	1080
詳細はこちら	1086
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy	1087
このポリシーを使用すると	1087
ポリシーの詳細	1087
ポリシーのバージョン	1087
JSON ポリシードキュメント	1087
詳細はこちら	1097
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy	1098
このポリシーを使用すると	1098
ポリシーの詳細	1098
ポリシーのバージョン	1098
JSON ポリシードキュメント	1098
詳細はこちら	1101
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy	1101
このポリシーを使用すると	1102
ポリシーの詳細	1102
ポリシーのバージョン	1102
JSON ポリシードキュメント	1102
詳細はこちら	1102

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy	1103
このポリシーを使用すると	1103
ポリシーの詳細	1103
ポリシーのバージョン	1103
JSON ポリシードキュメント	1104
詳細はこちら	1104
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy	1104
このポリシーを使用すると	1104
ポリシーの詳細	1105
ポリシーのバージョン	1105
JSON ポリシードキュメント	1105
詳細はこちら	1107
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy	1107
このポリシーを使用すると	1108
ポリシーの詳細	1108
ポリシーのバージョン	1108
JSON ポリシードキュメント	1108
詳細はこちら	1118
AmazonSecurityLakeAdministrator	1118
このポリシーを使用すると	1119
ポリシーの詳細	1119
ポリシーのバージョン	1119
JSON ポリシードキュメント	1119
詳細はこちら	1130
AmazonSecurityLakeMetastoreManager	1130
このポリシーを使用すると	1131
ポリシーの詳細	1131
ポリシーのバージョン	1131
JSON ポリシードキュメント	1131
詳細はこちら	1133
AmazonSecurityLakePermissionsBoundary	1134
このポリシーを使用すると	1134
ポリシーの詳細	1134
ポリシーのバージョン	1134
JSON ポリシードキュメント	1134
詳細はこちら	1137

AmazonSESEFullAccess	1138
このポリシーを使用すると	1138
ポリシーの詳細	1138
ポリシーのバージョン	1138
JSON ポリシードキュメント	1138
詳細はこちら	1139
AmazonSESReadOnlyAccess	1139
このポリシーを使用すると	1139
ポリシーの詳細	1139
ポリシーのバージョン	1139
JSON ポリシードキュメント	1140
詳細はこちら	1140
AmazonSESServiceRolePolicy	1140
このポリシーを使用すると	1140
ポリシーの詳細	1141
ポリシーのバージョン	1141
JSON ポリシードキュメント	1141
詳細はこちら	1142
AmazonSNSFullAccess	1142
このポリシーを使用すると	1142
ポリシーの詳細	1142
ポリシーのバージョン	1142
JSON ポリシードキュメント	1142
詳細はこちら	1143
AmazonSNSReadOnlyAccess	1143
このポリシーを使用すると	1143
ポリシーの詳細	1143
ポリシーのバージョン	1143
JSON ポリシードキュメント	1144
詳細はこちら	1144
AmazonSNSRole	1144
このポリシーを使用すると	1144
ポリシーの詳細	1144
ポリシーのバージョン	1145
JSON ポリシードキュメント	1145
詳細はこちら	1145

AmazonSQSFullAccess	1146
このポリシーを使用すると	1146
ポリシーの詳細	1146
ポリシーのバージョン	1146
JSON ポリシードキュメント	1146
詳細はこちら	1147
AmazonSQSReadOnlyAccess	1147
このポリシーを使用すると	1147
ポリシーの詳細	1147
ポリシーのバージョン	1147
JSON ポリシードキュメント	1147
詳細はこちら	1148
AmazonSSMAutomationApproverAccess	1148
このポリシーを使用すると	1148
ポリシーの詳細	1148
ポリシーのバージョン	1149
JSON ポリシードキュメント	1149
詳細はこちら	1149
AmazonSSMAutomationRole	1149
このポリシーを使用すると	1150
ポリシーの詳細	1150
ポリシーのバージョン	1150
JSON ポリシードキュメント	1150
詳細はこちら	1152
AmazonSSMDirectoryServiceAccess	1152
このポリシーを使用すると	1152
ポリシーの詳細	1152
ポリシーのバージョン	1152
JSON ポリシードキュメント	1152
詳細はこちら	1153
AmazonSSMFullAccess	1153
このポリシーを使用すると	1153
ポリシーの詳細	1153
ポリシーのバージョン	1154
JSON ポリシードキュメント	1154
詳細はこちら	1155

AmazonSSMMaintenanceWindowRole	1155
このポリシーを使用すると	1155
ポリシーの詳細	1155
ポリシーのバージョン	1156
JSON ポリシードキュメント	1156
詳細はこちら	1157
AmazonSSMManagedEC2InstanceDefaultPolicy	1157
このポリシーを使用すると	1158
ポリシーの詳細	1158
ポリシーのバージョン	1158
JSON ポリシードキュメント	1158
詳細はこちら	1159
AmazonSSMManagedInstanceCore	1159
このポリシーを使用すると	1160
ポリシーの詳細	1160
ポリシーのバージョン	1160
JSON ポリシードキュメント	1160
詳細はこちら	1161
AmazonSSMPatchAssociation	1161
このポリシーを使用すると	1162
ポリシーの詳細	1162
ポリシーのバージョン	1162
JSON ポリシードキュメント	1162
詳細はこちら	1163
AmazonSSMReadOnlyAccess	1163
このポリシーを使用すると	1163
ポリシーの詳細	1163
ポリシーのバージョン	1163
JSON ポリシードキュメント	1164
詳細はこちら	1164
AmazonSSMServiceRolePolicy	1164
このポリシーを使用すると	1164
ポリシーの詳細	1165
ポリシーのバージョン	1165
JSON ポリシードキュメント	1165
詳細はこちら	1170

AmazonSumerianFullAccess	1170
このポリシーを使用すると	1170
ポリシーの詳細	1170
ポリシーのバージョン	1171
JSON ポリシードキュメント	1171
詳細はこちら	1171
AmazonTextractFullAccess	1171
このポリシーを使用すると	1172
ポリシーの詳細	1172
ポリシーのバージョン	1172
JSON ポリシードキュメント	1172
詳細はこちら	1172
AmazonTextractServiceRole	1173
このポリシーを使用すると	1173
ポリシーの詳細	1173
ポリシーのバージョン	1173
JSON ポリシードキュメント	1173
詳細はこちら	1174
AmazonTimestreamConsoleFullAccess	1174
このポリシーを使用すると	1174
ポリシーの詳細	1174
ポリシーのバージョン	1174
JSON ポリシードキュメント	1175
詳細はこちら	1176
AmazonTimestreamFullAccess	1177
このポリシーを使用すると	1177
ポリシーの詳細	1177
ポリシーのバージョン	1177
JSON ポリシードキュメント	1177
詳細はこちら	1178
AmazonTimestreamInfluxDBFullAccess	1179
このポリシーを使用すると	1179
ポリシーの詳細	1179
ポリシーのバージョン	1179
JSON ポリシードキュメント	1179
詳細はこちら	1181

AmazonTimestreamInfluxDBServiceRolePolicy	1181
このポリシーを使用すると	1182
ポリシーの詳細	1182
ポリシーのバージョン	1182
JSON ポリシードキュメント	1182
詳細はこちら	1185
AmazonTimestreamReadOnlyAccess	1185
このポリシーを使用すると	1185
ポリシーの詳細	1185
ポリシーのバージョン	1185
JSON ポリシードキュメント	1185
詳細はこちら	1186
AmazonTranscribeFullAccess	1186
このポリシーを使用すると	1187
ポリシーの詳細	1187
ポリシーのバージョン	1187
JSON ポリシードキュメント	1187
詳細はこちら	1188
AmazonTranscribeReadOnlyAccess	1188
このポリシーを使用すると	1188
ポリシーの詳細	1188
ポリシーのバージョン	1188
JSON ポリシードキュメント	1189
詳細はこちら	1189
AmazonVPCCrossAccountNetworkInterfaceOperations	1189
このポリシーを使用すると	1189
ポリシーの詳細	1189
ポリシーのバージョン	1190
JSON ポリシードキュメント	1190
詳細はこちら	1191
AmazonVPCCrossAccountNetworkInterfaceOperations	1189
このポリシーを使用すると	1189
ポリシーの詳細	1189
ポリシーのバージョン	1190
JSON ポリシードキュメント	1190
詳細はこちら	1191
AmazonVPCFullAccess	1191
このポリシーを使用すると	1192
ポリシーの詳細	1192
ポリシーのバージョン	1192
JSON ポリシードキュメント	1192
詳細はこちら	1196

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy	1196
このポリシーを使用すると	1196
ポリシーの詳細	1196
ポリシーのバージョン	1197
JSON ポリシードキュメント	1197
詳細はこちら	1200
AmazonVPCReachabilityAnalyzerFullAccessPolicy	1200
このポリシーを使用すると	1201
ポリシーの詳細	1201
ポリシーのバージョン	1201
JSON ポリシードキュメント	1201
詳細はこちら	1204
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy	1204
このポリシーを使用すると	1205
ポリシーの詳細	1205
ポリシーのバージョン	1205
JSON ポリシードキュメント	1205
詳細はこちら	1206
AmazonVPCReadOnlyAccess	1206
このポリシーを使用すると	1206
ポリシーの詳細	1206
ポリシーのバージョン	1206
JSON ポリシードキュメント	1206
詳細はこちら	1208
AmazonWorkDocsFullAccess	1208
このポリシーを使用すると	1208
ポリシーの詳細	1208
ポリシーのバージョン	1208
JSON ポリシードキュメント	1209
詳細はこちら	1209
AmazonWorkDocsReadOnlyAccess	1209
このポリシーを使用すると	1209
ポリシーの詳細	1209
ポリシーのバージョン	1210
JSON ポリシードキュメント	1210
詳細はこちら	1210

AmazonWorkMailEventsServiceRolePolicy	1211
このポリシーを使用すると	1211
ポリシーの詳細	1211
ポリシーのバージョン	1211
JSON ポリシードキュメント	1211
詳細はこちら	1212
AmazonWorkMailFullAccess	1212
このポリシーを使用すると	1212
ポリシーの詳細	1212
ポリシーのバージョン	1212
JSON ポリシードキュメント	1213
詳細はこちら	1215
AmazonWorkMailMessageFlowFullAccess	1215
このポリシーを使用すると	1215
ポリシーの詳細	1215
ポリシーのバージョン	1215
JSON ポリシードキュメント	1215
詳細はこちら	1216
AmazonWorkMailMessageFlowReadOnlyAccess	1216
このポリシーを使用すると	1216
ポリシーの詳細	1216
ポリシーのバージョン	1217
JSON ポリシードキュメント	1217
詳細はこちら	1217
AmazonWorkMailReadOnlyAccess	1217
このポリシーを使用すると	1217
ポリシーの詳細	1218
ポリシーのバージョン	1218
JSON ポリシードキュメント	1218
詳細はこちら	1219
AmazonWorkSpacesAdmin	1219
このポリシーを使用すると	1219
ポリシーの詳細	1219
ポリシーのバージョン	1219
JSON ポリシードキュメント	1219
詳細はこちら	1220

AmazonWorkSpacesApplicationManagerAdminAccess	1221
このポリシーを使用すると	1221
ポリシーの詳細	1221
ポリシーのバージョン	1221
JSON ポリシードキュメント	1221
詳細はこちら	1222
AmazonWorkSpacesPCAAccess	1222
このポリシーを使用すると	1222
ポリシーの詳細	1222
ポリシーのバージョン	1222
JSON ポリシードキュメント	1223
詳細はこちら	1223
AmazonWorkSpacesSelfServiceAccess	1223
このポリシーを使用すると	1224
ポリシーの詳細	1224
ポリシーのバージョン	1224
JSON ポリシードキュメント	1224
詳細はこちら	1225
AmazonWorkSpacesServiceAccess	1225
このポリシーを使用すると	1225
ポリシーの詳細	1225
ポリシーのバージョン	1225
JSON ポリシードキュメント	1225
詳細はこちら	1226
AmazonWorkSpacesWebReadOnly	1226
このポリシーを使用すると	1226
ポリシーの詳細	1226
ポリシーのバージョン	1227
JSON ポリシードキュメント	1227
詳細はこちら	1228
AmazonWorkSpacesWebServiceRolePolicy	1228
このポリシーを使用すると	1228
ポリシーの詳細	1228
ポリシーのバージョン	1229
JSON ポリシードキュメント	1229
詳細はこちら	1231

AmazonZocaloFullAccess	1231
このポリシーを使用すると	1231
ポリシーの詳細	1231
ポリシーのバージョン	1232
JSON ポリシードキュメント	1232
詳細はこちら	1232
AmazonZocaloReadOnlyAccess	1233
このポリシーを使用すると	1233
ポリシーの詳細	1233
ポリシーのバージョン	1233
JSON ポリシードキュメント	1233
詳細はこちら	1234
AmplifyBackendDeployFullAccess	1234
このポリシーを使用すると	1234
ポリシーの詳細	1234
ポリシーのバージョン	1234
JSON ポリシードキュメント	1235
詳細はこちら	1238
APIGatewayServiceRolePolicy	1239
このポリシーを使用すると	1239
ポリシーの詳細	1239
ポリシーのバージョン	1239
JSON ポリシードキュメント	1239
詳細はこちら	1242
AppIntegrationsServiceLinkedRolePolicy	1242
このポリシーを使用すると	1242
ポリシーの詳細	1242
ポリシーのバージョン	1242
JSON ポリシードキュメント	1242
詳細はこちら	1244
ApplicationAutoScalingForAmazonAppStreamAccess	1244
このポリシーを使用すると	1244
ポリシーの詳細	1244
ポリシーのバージョン	1245
JSON ポリシードキュメント	1245
詳細はこちら	1245

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy	1246
このポリシーを使用すると	1246
ポリシーの詳細	1246
ポリシーのバージョン	1246
JSON ポリシードキュメント	1246
詳細はこちら	1248
AppRunnerNetworkingServiceRolePolicy	1249
このポリシーを使用すると	1249
ポリシーの詳細	1249
ポリシーのバージョン	1249
JSON ポリシードキュメント	1249
詳細はこちら	1251
AppRunnerServiceRolePolicy	1251
このポリシーを使用すると	1251
ポリシーの詳細	1251
ポリシーのバージョン	1251
JSON ポリシードキュメント	1251
詳細はこちら	1252
AutoScalingConsoleFullAccess	1253
このポリシーを使用すると	1253
ポリシーの詳細	1253
ポリシーのバージョン	1253
JSON ポリシードキュメント	1253
詳細はこちら	1255
AutoScalingConsoleReadOnlyAccess	1255
このポリシーを使用すると	1255
ポリシーの詳細	1255
ポリシーのバージョン	1256
JSON ポリシードキュメント	1256
詳細はこちら	1257
AutoScalingFullAccess	1257
このポリシーを使用すると	1257
ポリシーの詳細	1257
ポリシーのバージョン	1257
JSON ポリシードキュメント	1258
詳細はこちら	1259

AutoScalingNotificationAccessRole	1259
このポリシーを使用すると	1259
ポリシーの詳細	1259
ポリシーのバージョン	1260
JSON ポリシードキュメント	1260
詳細はこちら	1260
AutoScalingReadOnlyAccess	1260
このポリシーを使用すると	1261
ポリシーの詳細	1261
ポリシーのバージョン	1261
JSON ポリシードキュメント	1261
詳細はこちら	1261
AutoScalingServiceRolePolicy	1262
このポリシーを使用すると	1262
ポリシーの詳細	1262
ポリシーのバージョン	1262
JSON ポリシードキュメント	1262
詳細はこちら	1265
AWS_ConfigRole	1265
このポリシーを使用すると	1265
ポリシーの詳細	1266
ポリシーのバージョン	1266
JSON ポリシードキュメント	1266
詳細はこちら	1297
AWSAccountActivityAccess	1297
このポリシーを使用すると	1297
ポリシーの詳細	1297
ポリシーのバージョン	1297
JSON ポリシードキュメント	1298
詳細はこちら	1298
AWSAccountManagementFullAccess	1298
このポリシーを使用すると	1299
ポリシーの詳細	1299
ポリシーのバージョン	1299
JSON ポリシードキュメント	1299
詳細はこちら	1299

AWSAccountManagementReadOnlyAccess	1300
このポリシーを使用すると	1300
ポリシーの詳細	1300
ポリシーのバージョン	1300
JSON ポリシードキュメント	1300
詳細はこちら	1301
AWSAccountUsageReportAccess	1301
このポリシーを使用すると	1301
ポリシーの詳細	1301
ポリシーのバージョン	1301
JSON ポリシードキュメント	1302
詳細はこちら	1302
AWSAgentlessDiscoveryService	1302
このポリシーを使用すると	1302
ポリシーの詳細	1302
ポリシーのバージョン	1303
JSON ポリシードキュメント	1303
詳細はこちら	1305
AWSAppFabricFullAccess	1305
このポリシーを使用すると	1305
ポリシーの詳細	1305
ポリシーのバージョン	1305
JSON ポリシードキュメント	1306
詳細はこちら	1307
AWSAppFabricReadOnlyAccess	1307
このポリシーを使用すると	1307
ポリシーの詳細	1307
ポリシーのバージョン	1308
JSON ポリシードキュメント	1308
詳細はこちら	1308
AWSAppFabricServiceRolePolicy	1309
このポリシーを使用すると	1309
ポリシーの詳細	1309
ポリシーのバージョン	1309
JSON ポリシードキュメント	1309
詳細はこちら	1310

AWSApplicationAutoscalingAppStreamFleetPolicy	1311
このポリシーを使用すると	1311
ポリシーの詳細	1311
ポリシーのバージョン	1311
JSON ポリシードキュメント	1311
詳細はこちら	1312
AWSApplicationAutoscalingCassandraTablePolicy	1312
このポリシーを使用すると	1312
ポリシーの詳細	1312
ポリシーのバージョン	1313
JSON ポリシードキュメント	1313
詳細はこちら	1313
AWSApplicationAutoscalingComprehendEndpointPolicy	1314
このポリシーを使用すると	1314
ポリシーの詳細	1314
ポリシーのバージョン	1314
JSON ポリシードキュメント	1314
詳細はこちら	1315
AWSApplicationAutoScalingCustomResourcePolicy	1315
このポリシーを使用すると	1315
ポリシーの詳細	1315
ポリシーのバージョン	1316
JSON ポリシードキュメント	1316
詳細はこちら	1316
AWSApplicationAutoscalingDynamoDBTablePolicy	1316
このポリシーを使用すると	1317
ポリシーの詳細	1317
ポリシーのバージョン	1317
JSON ポリシードキュメント	1317
詳細はこちら	1318
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy	1318
このポリシーを使用すると	1318
ポリシーの詳細	1318
ポリシーのバージョン	1318
JSON ポリシードキュメント	1319
詳細はこちら	1319

AWSApplicationAutoscalingECSServicePolicy	1319
このポリシーを使用すると	1319
ポリシーの詳細	1320
ポリシーのバージョン	1320
JSON ポリシードキュメント	1320
詳細はこちら	1321
AWSApplicationAutoscalingElastiCacheRGPolicy	1321
このポリシーを使用すると	1321
ポリシーの詳細	1321
ポリシーのバージョン	1321
JSON ポリシードキュメント	1321
詳細はこちら	1322
AWSApplicationAutoscalingEMRInstanceGroupPolicy	1322
このポリシーを使用すると	1323
ポリシーの詳細	1323
ポリシーのバージョン	1323
JSON ポリシードキュメント	1323
詳細はこちら	1324
AWSApplicationAutoscalingKafkaClusterPolicy	1324
このポリシーを使用すると	1324
ポリシーの詳細	1324
ポリシーのバージョン	1324
JSON ポリシードキュメント	1325
詳細はこちら	1325
AWSApplicationAutoscalingLambdaConcurrencyPolicy	1325
このポリシーを使用すると	1325
ポリシーの詳細	1326
ポリシーのバージョン	1326
JSON ポリシードキュメント	1326
詳細はこちら	1327
AWSApplicationAutoscalingNeptuneClusterPolicy	1327
このポリシーを使用すると	1327
ポリシーの詳細	1327
ポリシーのバージョン	1327
JSON ポリシードキュメント	1327
詳細はこちら	1329

AWSApplicationAutoscalingRDSClusterPolicy	1329
このポリシーを使用すると	1329
ポリシーの詳細	1329
ポリシーのバージョン	1330
JSON ポリシードキュメント	1330
詳細はこちら	1331
AWSApplicationAutoscalingSageMakerEndpointPolicy	1331
このポリシーを使用すると	1331
ポリシーの詳細	1331
ポリシーのバージョン	1331
JSON ポリシードキュメント	1332
詳細はこちら	1332
AWSApplicationDiscoveryAgentAccess	1333
このポリシーを使用すると	1333
ポリシーの詳細	1333
ポリシーのバージョン	1333
JSON ポリシードキュメント	1333
詳細はこちら	1334
AWSApplicationDiscoveryAgentlessCollectorAccess	1334
このポリシーを使用すると	1334
ポリシーの詳細	1334
ポリシーのバージョン	1335
JSON ポリシードキュメント	1335
詳細はこちら	1336
AWSApplicationDiscoveryServiceFullAccess	1336
このポリシーを使用すると	1336
ポリシーの詳細	1336
ポリシーのバージョン	1337
JSON ポリシードキュメント	1337
詳細はこちら	1338
AWSApplicationMigrationAgentInstallationPolicy	1338
このポリシーを使用すると	1339
ポリシーの詳細	1339
ポリシーのバージョン	1339
JSON ポリシードキュメント	1339
詳細はこちら	1340

AWSApplicationMigrationAgentPolicy	1340
このポリシーを使用すると	1340
ポリシーの詳細	1341
ポリシーのバージョン	1341
JSON ポリシードキュメント	1341
詳細はこちら	1342
AWSApplicationMigrationAgentPolicy_v2	1342
このポリシーを使用すると	1342
ポリシーの詳細	1342
ポリシーのバージョン	1343
JSON ポリシードキュメント	1343
詳細はこちら	1343
AWSApplicationMigrationConversionServerPolicy	1344
このポリシーを使用すると	1344
ポリシーの詳細	1344
ポリシーのバージョン	1344
JSON ポリシードキュメント	1345
詳細はこちら	1345
AWSApplicationMigrationEC2Access	1345
このポリシーを使用すると	1345
ポリシーの詳細	1346
ポリシーのバージョン	1346
JSON ポリシードキュメント	1346
詳細はこちら	1354
AWSApplicationMigrationFullAccess	1354
このポリシーを使用すると	1354
ポリシーの詳細	1354
ポリシーのバージョン	1354
JSON ポリシードキュメント	1355
詳細はこちら	1361
AWSApplicationMigrationMGHAccess	1361
このポリシーを使用すると	1361
ポリシーの詳細	1361
ポリシーのバージョン	1361
JSON ポリシードキュメント	1362
詳細はこちら	1362

AWSApplicationMigrationReadOnlyAccess	1362
このポリシーを使用すると	1363
ポリシーの詳細	1363
ポリシーのバージョン	1363
JSON ポリシードキュメント	1363
詳細はこちら	1364
AWSApplicationMigrationReplicationServerPolicy	1364
このポリシーを使用すると	1365
ポリシーの詳細	1365
ポリシーのバージョン	1365
JSON ポリシードキュメント	1365
詳細はこちら	1367
AWSApplicationMigrationServiceEc2InstancePolicy	1367
このポリシーを使用すると	1367
ポリシーの詳細	1367
ポリシーのバージョン	1368
JSON ポリシードキュメント	1368
詳細はこちら	1369
AWSApplicationMigrationServiceRolePolicy	1369
このポリシーを使用すると	1369
ポリシーの詳細	1370
ポリシーのバージョン	1370
JSON ポリシードキュメント	1370
詳細はこちら	1377
AWSApplicationMigrationSSMAccess	1377
このポリシーを使用すると	1377
ポリシーの詳細	1377
ポリシーのバージョン	1378
JSON ポリシードキュメント	1378
詳細はこちら	1380
AWSApplicationMigrationVCenterClientPolicy	1380
このポリシーを使用すると	1380
ポリシーの詳細	1380
ポリシーのバージョン	1380
JSON ポリシードキュメント	1381
詳細はこちら	1381

AWSAppMeshEnvoyAccess	1382
このポリシーを使用すると	1382
ポリシーの詳細	1382
ポリシーのバージョン	1382
JSON ポリシードキュメント	1382
詳細はこちら	1383
AWSAppMeshFullAccess	1383
このポリシーを使用すると	1383
ポリシーの詳細	1383
ポリシーのバージョン	1383
JSON ポリシードキュメント	1383
詳細はこちら	1385
AWSAppMeshPreviewEnvoyAccess	1385
このポリシーを使用すると	1385
ポリシーの詳細	1385
ポリシーのバージョン	1385
JSON ポリシードキュメント	1386
詳細はこちら	1386
AWSAppMeshPreviewServiceRolePolicy	1386
このポリシーを使用すると	1386
ポリシーの詳細	1387
ポリシーのバージョン	1387
JSON ポリシードキュメント	1387
詳細はこちら	1388
AWSAppMeshReadOnly	1388
このポリシーを使用すると	1388
ポリシーの詳細	1388
ポリシーのバージョン	1388
JSON ポリシードキュメント	1388
詳細はこちら	1389
AWSAppMeshServiceRolePolicy	1390
このポリシーを使用すると	1390
ポリシーの詳細	1390
ポリシーのバージョン	1390
JSON ポリシードキュメント	1390
詳細はこちら	1391

AWSAppRunnerFullAccess	1391
このポリシーを使用すると	1391
ポリシーの詳細	1391
ポリシーのバージョン	1391
JSON ポリシードキュメント	1392
詳細はこちら	1392
AWSAppRunnerReadOnlyAccess	1393
このポリシーを使用すると	1393
ポリシーの詳細	1393
ポリシーのバージョン	1393
JSON ポリシードキュメント	1393
詳細はこちら	1394
AWSAppRunnerServicePolicyForECRAccess	1394
このポリシーを使用すると	1394
ポリシーの詳細	1394
ポリシーのバージョン	1395
JSON ポリシードキュメント	1395
詳細はこちら	1395
AWSAppSyncAdministrator	1395
このポリシーを使用すると	1396
ポリシーの詳細	1396
ポリシーのバージョン	1396
JSON ポリシードキュメント	1396
詳細はこちら	1397
AWSAppSyncInvokeFullAccess	1397
このポリシーを使用すると	1398
ポリシーの詳細	1398
ポリシーのバージョン	1398
JSON ポリシードキュメント	1398
詳細はこちら	1399
AWSAppSyncPushToCloudWatchLogs	1399
このポリシーを使用すると	1399
ポリシーの詳細	1399
ポリシーのバージョン	1399
JSON ポリシードキュメント	1399
詳細はこちら	1400

AWSAppSyncSchemaAuthor	1400
このポリシーを使用すると	1400
ポリシーの詳細	1400
ポリシーのバージョン	1401
JSON ポリシードキュメント	1401
詳細はこちら	1402
AWSAppSyncServiceRolePolicy	1402
このポリシーを使用すると	1402
ポリシーの詳細	1402
ポリシーのバージョン	1402
JSON ポリシードキュメント	1403
詳細はこちら	1403
AWSArtifactAccountSync	1403
このポリシーを使用すると	1403
ポリシーの詳細	1404
ポリシーのバージョン	1404
JSON ポリシードキュメント	1404
詳細はこちら	1404
AWSArtifactReportsReadOnlyAccess	1405
このポリシーを使用すると	1405
ポリシーの詳細	1405
ポリシーのバージョン	1405
JSON ポリシードキュメント	1405
詳細はこちら	1406
AWSArtifactServiceRolePolicy	1406
このポリシーを使用すると	1406
ポリシーの詳細	1406
ポリシーのバージョン	1406
JSON ポリシードキュメント	1407
詳細はこちら	1407
AWSAuditManagerAdministratorAccess	1407
このポリシーを使用すると	1407
ポリシーの詳細	1408
ポリシーのバージョン	1408
JSON ポリシードキュメント	1408
詳細はこちら	1412

AWSAuditManagerServiceRolePolicy	1412
このポリシーを使用すると	1412
ポリシーの詳細	1412
ポリシーのバージョン	1413
JSON ポリシードキュメント	1413
詳細はこちら	1420
AWSAutoScalingPlansEC2AutoScalingPolicy	1420
このポリシーを使用すると	1420
ポリシーの詳細	1420
ポリシーのバージョン	1420
JSON ポリシードキュメント	1421
詳細はこちら	1421
AWSBackupAuditAccess	1421
このポリシーを使用すると	1421
ポリシーの詳細	1422
ポリシーのバージョン	1422
JSON ポリシードキュメント	1422
詳細はこちら	1423
AWSBackupDataTransferAccess	1423
このポリシーを使用すると	1424
ポリシーの詳細	1424
ポリシーのバージョン	1424
JSON ポリシードキュメント	1424
詳細はこちら	1425
AWSBackupFullAccess	1425
このポリシーを使用すると	1425
ポリシーの詳細	1425
ポリシーのバージョン	1425
JSON ポリシードキュメント	1426
詳細はこちら	1435
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync	1436
このポリシーを使用すると	1436
ポリシーの詳細	1436
ポリシーのバージョン	1436
JSON ポリシードキュメント	1436
詳細はこちら	1437

AWSBackupOperatorAccess	1437
このポリシーを使用すると	1437
ポリシーの詳細	1437
ポリシーのバージョン	1438
JSON ポリシードキュメント	1438
詳細はこちら	1445
AWSBackupOrganizationAdminAccess	1445
このポリシーを使用すると	1445
ポリシーの詳細	1445
ポリシーのバージョン	1445
JSON ポリシードキュメント	1446
詳細はこちら	1447
AWSBackupRestoreAccessForSAPHANA	1448
このポリシーを使用すると	1448
ポリシーの詳細	1448
ポリシーのバージョン	1448
JSON ポリシードキュメント	1448
詳細はこちら	1449
AWSBackupServiceLinkedRolePolicyForBackup	1449
このポリシーを使用すると	1450
ポリシーの詳細	1450
ポリシーのバージョン	1450
JSON ポリシードキュメント	1450
詳細はこちら	1458
AWSBackupServiceLinkedRolePolicyForBackupTest	1458
このポリシーを使用すると	1458
ポリシーの詳細	1459
ポリシーのバージョン	1459
JSON ポリシードキュメント	1459
詳細はこちら	1460
AWSBackupServiceRolePolicyForBackup	1460
このポリシーを使用すると	1460
ポリシーの詳細	1460
ポリシーのバージョン	1460
JSON ポリシードキュメント	1461
詳細はこちら	1471

AWSBackupServiceRolePolicyForRestores	1472
このポリシーを使用すると	1472
ポリシーの詳細	1472
ポリシーのバージョン	1472
JSON ポリシードキュメント	1472
詳細はこちら	1482
AWSBackupServiceRolePolicyForS3Backup	1483
このポリシーを使用すると	1483
ポリシーの詳細	1483
ポリシーのバージョン	1483
JSON ポリシードキュメント	1483
詳細はこちら	1486
AWSBackupServiceRolePolicyForS3Restore	1486
このポリシーを使用すると	1486
ポリシーの詳細	1486
ポリシーのバージョン	1486
JSON ポリシードキュメント	1487
詳細はこちら	1488
AWSBatchFullAccess	1488
このポリシーを使用すると	1488
ポリシーの詳細	1488
ポリシーのバージョン	1489
JSON ポリシードキュメント	1489
詳細はこちら	1490
AWSBatchServiceEventTargetRole	1490
このポリシーを使用すると	1491
ポリシーの詳細	1491
ポリシーのバージョン	1491
JSON ポリシードキュメント	1491
詳細はこちら	1491
AWSBatchServiceRole	1492
このポリシーを使用すると	1492
ポリシーの詳細	1492
ポリシーのバージョン	1492
JSON ポリシードキュメント	1492
詳細はこちら	1495

AWSBCMDDataExportsServiceRolePolicy	1496
このポリシーを使用すると	1496
ポリシーの詳細	1496
ポリシーのバージョン	1496
JSON ポリシードキュメント	1496
詳細はこちら	1497
AWSBillingConductorFullAccess	1497
このポリシーを使用すると	1497
ポリシーの詳細	1497
ポリシーのバージョン	1497
JSON ポリシードキュメント	1498
詳細はこちら	1498
AWSBillingConductorReadOnlyAccess	1498
このポリシーを使用すると	1499
ポリシーの詳細	1499
ポリシーのバージョン	1499
JSON ポリシードキュメント	1499
詳細はこちら	1500
AWSBillingReadOnlyAccess	1500
このポリシーを使用すると	1500
ポリシーの詳細	1500
ポリシーのバージョン	1500
JSON ポリシードキュメント	1500
詳細はこちら	1502
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM	1502
このポリシーを使用すると	1502
ポリシーの詳細	1502
ポリシーのバージョン	1503
JSON ポリシードキュメント	1503
詳細はこちら	1504
AWSBudgetsActionsWithAWSResourceControlAccess	1504
このポリシーを使用すると	1504
ポリシーの詳細	1504
ポリシーのバージョン	1505
JSON ポリシードキュメント	1505
詳細はこちら	1506

AWSBudgetsReadOnlyAccess	1506
このポリシーを使用すると	1506
ポリシーの詳細	1506
ポリシーのバージョン	1507
JSON ポリシードキュメント	1507
詳細はこちら	1507
AWSBugBustFullAccess	1508
このポリシーを使用すると	1508
ポリシーの詳細	1508
ポリシーのバージョン	1508
JSON ポリシードキュメント	1508
詳細はこちら	1509
AWSBugBustPlayerAccess	1510
このポリシーを使用すると	1510
ポリシーの詳細	1510
ポリシーのバージョン	1510
JSON ポリシードキュメント	1510
詳細はこちら	1511
AWSBugBustServiceRolePolicy	1511
このポリシーを使用すると	1512
ポリシーの詳細	1512
ポリシーのバージョン	1512
JSON ポリシードキュメント	1512
詳細はこちら	1513
AWSCertificateManagerFullAccess	1513
このポリシーを使用すると	1513
ポリシーの詳細	1513
ポリシーのバージョン	1513
JSON ポリシードキュメント	1514
詳細はこちら	1514
AWSCertificateManagerPrivateCAAuditor	1515
このポリシーを使用すると	1515
ポリシーの詳細	1515
ポリシーのバージョン	1515
JSON ポリシードキュメント	1515
詳細はこちら	1516

AWSCertificateManagerPrivateCAFullAccess	1516
このポリシーを使用すると	1516
ポリシーの詳細	1516
ポリシーのバージョン	1517
JSON ポリシードキュメント	1517
詳細はこちら	1517
AWSCertificateManagerPrivateCAPrivilegedUser	1517
このポリシーを使用すると	1518
ポリシーの詳細	1518
ポリシーのバージョン	1518
JSON ポリシードキュメント	1518
詳細はこちら	1519
AWSCertificateManagerPrivateCAReadOnly	1520
このポリシーを使用すると	1520
ポリシーの詳細	1520
ポリシーのバージョン	1520
JSON ポリシードキュメント	1520
詳細はこちら	1521
AWSCertificateManagerPrivateCAUser	1521
このポリシーを使用すると	1521
ポリシーの詳細	1521
ポリシーのバージョン	1521
JSON ポリシードキュメント	1522
詳細はこちら	1523
AWSCertificateManagerReadOnly	1523
このポリシーを使用すると	1523
ポリシーの詳細	1523
ポリシーのバージョン	1524
JSON ポリシードキュメント	1524
詳細はこちら	1524
AWSChatbotServiceLinkedRolePolicy	1524
このポリシーを使用すると	1525
ポリシーの詳細	1525
ポリシーのバージョン	1525
JSON ポリシードキュメント	1525
詳細はこちら	1526

AWSCleanRoomsFullAccess	1526
このポリシーを使用すると	1526
ポリシーの詳細	1526
ポリシーのバージョン	1526
JSON ポリシードキュメント	1527
詳細はこちら	1531
AWSCleanRoomsFullAccessNoQuerying	1531
このポリシーを使用すると	1531
ポリシーの詳細	1532
ポリシーのバージョン	1532
JSON ポリシードキュメント	1532
詳細はこちら	1537
AWSCleanRoomsMLFullAccess	1537
このポリシーを使用すると	1537
ポリシーの詳細	1537
ポリシーのバージョン	1537
JSON ポリシードキュメント	1538
詳細はこちら	1541
AWSCleanRoomsMLReadOnlyAccess	1541
このポリシーを使用すると	1542
ポリシーの詳細	1542
ポリシーのバージョン	1542
JSON ポリシードキュメント	1542
詳細はこちら	1543
AWSCleanRoomsReadOnlyAccess	1543
このポリシーを使用すると	1543
ポリシーの詳細	1543
ポリシーのバージョン	1544
JSON ポリシードキュメント	1544
詳細はこちら	1545
AWSCloud9Administrator	1545
このポリシーを使用すると	1545
ポリシーの詳細	1545
ポリシーのバージョン	1546
JSON ポリシードキュメント	1546
詳細はこちら	1547

AWSCloud9EnvironmentMember	1547
このポリシーを使用すると	1548
ポリシーの詳細	1548
ポリシーのバージョン	1548
JSON ポリシードキュメント	1548
詳細はこちら	1549
AWSCloud9ServiceRolePolicy	1550
このポリシーを使用すると	1550
ポリシーの詳細	1550
ポリシーのバージョン	1550
JSON ポリシードキュメント	1550
詳細はこちら	1553
AWSCloud9SSMInstanceProfile	1553
このポリシーを使用すると	1553
ポリシーの詳細	1553
ポリシーのバージョン	1553
JSON ポリシードキュメント	1554
詳細はこちら	1554
AWSCloud9User	1554
このポリシーを使用すると	1554
ポリシーの詳細	1554
ポリシーのバージョン	1555
JSON ポリシードキュメント	1555
詳細はこちら	1557
AWSCloudFormationFullAccess	1557
このポリシーを使用すると	1558
ポリシーの詳細	1558
ポリシーのバージョン	1558
JSON ポリシードキュメント	1558
詳細はこちら	1558
AWSCloudFormationReadOnlyAccess	1559
このポリシーを使用すると	1559
ポリシーの詳細	1559
ポリシーのバージョン	1559
JSON ポリシードキュメント	1559
詳細はこちら	1560

AWSCloudFrontLogger	1560
このポリシーを使用すると	1560
ポリシーの詳細	1560
ポリシーのバージョン	1560
JSON ポリシードキュメント	1561
詳細はこちら	1561
AWSCloudHSMFullAccess	1561
このポリシーを使用すると	1561
ポリシーの詳細	1561
ポリシーのバージョン	1562
JSON ポリシードキュメント	1562
詳細はこちら	1562
AWSCloudHSMReadOnlyAccess	1562
このポリシーを使用すると	1563
ポリシーの詳細	1563
ポリシーのバージョン	1563
JSON ポリシードキュメント	1563
詳細はこちら	1563
AWSCloudHSMRole	1564
このポリシーを使用すると	1564
ポリシーの詳細	1564
ポリシーのバージョン	1564
JSON ポリシードキュメント	1564
詳細はこちら	1565
AWSCloudMapDiscoverInstanceAccess	1565
このポリシーを使用すると	1565
ポリシーの詳細	1565
ポリシーのバージョン	1566
JSON ポリシードキュメント	1566
詳細はこちら	1566
AWSCloudMapFullAccess	1566
このポリシーを使用すると	1567
ポリシーの詳細	1567
ポリシーのバージョン	1567
JSON ポリシードキュメント	1567
詳細はこちら	1568

AWSCloudMapReadOnlyAccess	1568
このポリシーを使用すると	1568
ポリシーの詳細	1568
ポリシーのバージョン	1568
JSON ポリシードキュメント	1569
詳細はこちら	1569
AWSCloudMapRegisterInstanceAccess	1569
このポリシーを使用すると	1570
ポリシーの詳細	1570
ポリシーのバージョン	1570
JSON ポリシードキュメント	1570
詳細はこちら	1571
AWSCloudShellFullAccess	1571
このポリシーを使用すると	1571
ポリシーの詳細	1571
ポリシーのバージョン	1571
JSON ポリシードキュメント	1572
詳細はこちら	1572
AWSCloudTrail_FullAccess	1572
このポリシーを使用すると	1572
ポリシーの詳細	1572
ポリシーのバージョン	1573
JSON ポリシードキュメント	1573
詳細はこちら	1575
AWSCloudTrail_ReadOnlyAccess	1576
このポリシーを使用すると	1576
ポリシーの詳細	1576
ポリシーのバージョン	1576
JSON ポリシードキュメント	1576
詳細はこちら	1577
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy	1577
このポリシーを使用すると	1577
ポリシーの詳細	1577
ポリシーのバージョン	1578
JSON ポリシードキュメント	1578
詳細はこちら	1578

AWSCodeArtifactAdminAccess	1578
このポリシーを使用すると	1578
ポリシーの詳細	1578
ポリシーのバージョン	1579
JSON ポリシードキュメント	1579
詳細はこちら	1579
AWSCodeArtifactReadOnlyAccess	1580
このポリシーを使用すると	1580
ポリシーの詳細	1580
ポリシーのバージョン	1580
JSON ポリシードキュメント	1580
詳細はこちら	1581
AWSCodeBuildAdminAccess	1581
このポリシーを使用すると	1581
ポリシーの詳細	1582
ポリシーのバージョン	1582
JSON ポリシードキュメント	1582
詳細はこちら	1585
AWSCodeBuildDeveloperAccess	1586
このポリシーを使用すると	1586
ポリシーの詳細	1586
ポリシーのバージョン	1586
JSON ポリシードキュメント	1586
詳細はこちら	1589
AWSCodeBuildReadOnlyAccess	1589
このポリシーを使用すると	1589
ポリシーの詳細	1589
ポリシーのバージョン	1590
JSON ポリシードキュメント	1590
詳細はこちら	1591
AWSCodeCommitFullAccess	1591
このポリシーを使用すると	1592
ポリシーの詳細	1592
ポリシーのバージョン	1592
JSON ポリシードキュメント	1592
詳細はこちら	1597

AWSCodeCommitPowerUser	1597
このポリシーを使用すると	1597
ポリシーの詳細	1597
ポリシーのバージョン	1597
JSON ポリシードキュメント	1598
詳細はこちら	1602
AWSCodeCommitReadOnly	1603
このポリシーを使用すると	1603
ポリシーの詳細	1603
ポリシーのバージョン	1603
JSON ポリシードキュメント	1603
詳細はこちら	1606
AWSCodeDeployDeployerAccess	1606
このポリシーを使用すると	1606
ポリシーの詳細	1606
ポリシーのバージョン	1606
JSON ポリシードキュメント	1607
詳細はこちら	1608
AWSCodeDeployFullAccess	1608
このポリシーを使用すると	1608
ポリシーの詳細	1609
ポリシーのバージョン	1609
JSON ポリシードキュメント	1609
詳細はこちら	1611
AWSCodeDeployReadOnlyAccess	1611
このポリシーを使用すると	1611
ポリシーの詳細	1611
ポリシーのバージョン	1611
JSON ポリシードキュメント	1611
詳細はこちら	1612
AWSCodeDeployRole	1613
このポリシーを使用すると	1613
ポリシーの詳細	1613
ポリシーのバージョン	1613
JSON ポリシードキュメント	1613
詳細はこちら	1614

AWSCodeDeployRoleForCloudFormation	1615
このポリシーを使用すると	1615
ポリシーの詳細	1615
ポリシーのバージョン	1615
JSON ポリシードキュメント	1615
詳細はこちら	1616
AWSCodeDeployRoleForECS	1616
このポリシーを使用すると	1616
ポリシーの詳細	1616
ポリシーのバージョン	1617
JSON ポリシードキュメント	1617
詳細はこちら	1618
AWSCodeDeployRoleForECSLimited	1618
このポリシーを使用すると	1618
ポリシーの詳細	1618
ポリシーのバージョン	1618
JSON ポリシードキュメント	1619
詳細はこちら	1620
AWSCodeDeployRoleForLambda	1621
このポリシーを使用すると	1621
ポリシーの詳細	1621
ポリシーのバージョン	1621
JSON ポリシードキュメント	1621
詳細はこちら	1622
AWSCodeDeployRoleForLambdaLimited	1623
このポリシーを使用すると	1623
ポリシーの詳細	1623
ポリシーのバージョン	1623
JSON ポリシードキュメント	1623
詳細はこちら	1624
AWSCodePipeline_FullAccess	1625
このポリシーを使用すると	1625
ポリシーの詳細	1625
ポリシーのバージョン	1625
JSON ポリシードキュメント	1625
詳細はこちら	1629

AWSCodePipeline_ReadOnlyAccess	1629
このポリシーを使用すると	1629
ポリシーの詳細	1629
ポリシーのバージョン	1630
JSON ポリシードキュメント	1630
詳細はこちら	1631
AWSCodePipelineApproverAccess	1631
このポリシーを使用すると	1631
ポリシーの詳細	1631
ポリシーのバージョン	1632
JSON ポリシードキュメント	1632
詳細はこちら	1632
AWSCodePipelineCustomActionAccess	1632
このポリシーを使用すると	1633
ポリシーの詳細	1633
ポリシーのバージョン	1633
JSON ポリシードキュメント	1633
詳細はこちら	1634
AWSCodeStarFullAccess	1634
このポリシーを使用すると	1634
ポリシーの詳細	1634
ポリシーのバージョン	1634
JSON ポリシードキュメント	1634
詳細はこちら	1635
AWSCodeStarNotificationsServiceRolePolicy	1635
このポリシーを使用すると	1636
ポリシーの詳細	1636
ポリシーのバージョン	1636
JSON ポリシードキュメント	1636
詳細はこちら	1637
AWSCodeStarServiceRole	1637
このポリシーを使用すると	1638
ポリシーの詳細	1638
ポリシーのバージョン	1638
JSON ポリシードキュメント	1638
詳細はこちら	1643

AWSCompromisedKeyQuarantine	1643
このポリシーを使用すると	1643
ポリシーの詳細	1643
ポリシーのバージョン	1644
JSON ポリシードキュメント	1644
詳細はこちら	1645
AWSCompromisedKeyQuarantineV2	1645
このポリシーを使用すると	1645
ポリシーの詳細	1645
ポリシーのバージョン	1645
JSON ポリシードキュメント	1646
詳細はこちら	1647
AWSConfigMultiAccountSetupPolicy	1648
このポリシーを使用すると	1648
ポリシーの詳細	1648
ポリシーのバージョン	1648
JSON ポリシードキュメント	1648
詳細はこちら	1650
AWSConfigRemediationServiceRolePolicy	1650
このポリシーを使用すると	1651
ポリシーの詳細	1651
ポリシーのバージョン	1651
JSON ポリシードキュメント	1651
詳細はこちら	1652
AWSConfigRoleForOrganizations	1652
このポリシーを使用すると	1652
ポリシーの詳細	1652
ポリシーのバージョン	1652
JSON ポリシードキュメント	1653
詳細はこちら	1653
AWSConfigRulesExecutionRole	1653
このポリシーを使用すると	1653
ポリシーの詳細	1654
ポリシーのバージョン	1654
JSON ポリシードキュメント	1654
詳細はこちら	1655

AWSConfigServiceRolePolicy	1655
このポリシーを使用すると	1655
ポリシーの詳細	1655
ポリシーのバージョン	1655
JSON ポリシードキュメント	1656
詳細はこちら	1687
AWSConfigUserAccess	1687
このポリシーを使用すると	1687
ポリシーの詳細	1687
ポリシーのバージョン	1688
JSON ポリシードキュメント	1688
詳細はこちら	1688
AWSConnector	1689
このポリシーを使用すると	1689
ポリシーの詳細	1689
ポリシーのバージョン	1689
JSON ポリシードキュメント	1689
詳細はこちら	1691
AWSControlTowerAccountServiceRolePolicy	1691
このポリシーを使用すると	1692
ポリシーの詳細	1692
ポリシーのバージョン	1692
JSON ポリシードキュメント	1692
詳細はこちら	1694
AWSControlTowerServiceRolePolicy	1694
このポリシーを使用すると	1694
ポリシーの詳細	1694
ポリシーのバージョン	1694
JSON ポリシードキュメント	1695
詳細はこちら	1699
AWSCostAndUsageReportAutomationPolicy	1699
このポリシーを使用すると	1700
ポリシーの詳細	1700
ポリシーのバージョン	1700
JSON ポリシードキュメント	1700
詳細はこちら	1701

AWSDataExchangeFullAccess	1701
このポリシーを使用すると	1701
ポリシーの詳細	1702
ポリシーのバージョン	1702
JSON ポリシードキュメント	1702
詳細はこちら	1705
AWSDataExchangeProviderFullAccess	1706
このポリシーを使用すると	1706
ポリシーの詳細	1706
ポリシーのバージョン	1706
JSON ポリシードキュメント	1706
詳細はこちら	1710
AWSDataExchangeReadOnly	1710
このポリシーを使用すると	1710
ポリシーの詳細	1710
ポリシーのバージョン	1711
JSON ポリシードキュメント	1711
詳細はこちら	1712
AWSDataExchangeSubscriberFullAccess	1712
このポリシーを使用すると	1712
ポリシーの詳細	1712
ポリシーのバージョン	1712
JSON ポリシードキュメント	1713
詳細はこちら	1715
AWSDataLifecycleManagerServiceRole	1715
このポリシーを使用すると	1715
ポリシーの詳細	1715
ポリシーのバージョン	1715
JSON ポリシードキュメント	1716
詳細はこちら	1717
AWSDataLifecycleManagerServiceRoleForAMIManagement	1717
このポリシーを使用すると	1717
ポリシーの詳細	1717
ポリシーのバージョン	1718
JSON ポリシードキュメント	1718
詳細はこちら	1719

AWSDataLifecycleManagerSSMFullAccess	1719
このポリシーを使用すると	1719
ポリシーの詳細	1719
ポリシーのバージョン	1720
JSON ポリシードキュメント	1720
詳細はこちら	1721
AWSDataPipeline_FullAccess	1722
このポリシーを使用すると	1722
ポリシーの詳細	1722
ポリシーのバージョン	1722
JSON ポリシードキュメント	1722
詳細はこちら	1723
AWSDataPipeline_PowerUser	1723
このポリシーを使用すると	1723
ポリシーの詳細	1724
ポリシーのバージョン	1724
JSON ポリシードキュメント	1724
詳細はこちら	1725
AWSDataSyncDiscoveryServiceRolePolicy	1725
このポリシーを使用すると	1725
ポリシーの詳細	1725
ポリシーのバージョン	1726
JSON ポリシードキュメント	1726
詳細はこちら	1727
AWSDataSyncFullAccess	1727
このポリシーを使用すると	1727
ポリシーの詳細	1727
ポリシーのバージョン	1727
JSON ポリシードキュメント	1728
詳細はこちら	1729
AWSDataSyncReadOnlyAccess	1729
このポリシーを使用すると	1729
ポリシーの詳細	1729
ポリシーのバージョン	1730
JSON ポリシードキュメント	1730
詳細はこちら	1730

AWSDeadlineCloud-FleetWorker	1731
このポリシーを使用すると	1731
ポリシーの詳細	1731
ポリシーのバージョン	1731
JSON ポリシードキュメント	1731
詳細はこちら	1732
AWSDeadlineCloud-UserAccessFarms	1732
このポリシーを使用すると	1732
ポリシーの詳細	1732
ポリシーのバージョン	1733
JSON ポリシードキュメント	1733
詳細はこちら	1738
AWSDeadlineCloud-UserAccessFleets	1738
このポリシーを使用すると	1738
ポリシーの詳細	1738
ポリシーのバージョン	1739
JSON ポリシードキュメント	1739
詳細はこちら	1742
AWSDeadlineCloud-UserAccessJobs	1743
このポリシーを使用すると	1743
ポリシーの詳細	1743
ポリシーのバージョン	1743
JSON ポリシードキュメント	1743
詳細はこちら	1747
AWSDeadlineCloud-UserAccessQueues	1747
このポリシーを使用すると	1748
ポリシーの詳細	1748
ポリシーのバージョン	1748
JSON ポリシードキュメント	1748
詳細はこちら	1753
AWSDeadlineCloud-WorkerHost	1753
このポリシーを使用すると	1753
ポリシーの詳細	1753
ポリシーのバージョン	1753
JSON ポリシードキュメント	1754
詳細はこちら	1754

AWSDeepLensLambdaFunctionAccessPolicy	1754
このポリシーを使用すると	1755
ポリシーの詳細	1755
ポリシーのバージョン	1755
JSON ポリシードキュメント	1755
詳細はこちら	1756
AWSDeepLensServiceRolePolicy	1757
このポリシーを使用すると	1757
ポリシーの詳細	1757
ポリシーのバージョン	1757
JSON ポリシードキュメント	1757
詳細はこちら	1764
AWSDeepRacerAccountAdminAccess	1765
このポリシーを使用すると	1765
ポリシーの詳細	1765
ポリシーのバージョン	1765
JSON ポリシードキュメント	1765
詳細はこちら	1766
AWSDeepRacerCloudFormationAccessPolicy	1766
このポリシーを使用すると	1766
ポリシーの詳細	1766
ポリシーのバージョン	1766
JSON ポリシードキュメント	1767
詳細はこちら	1770
AWSDeepRacerDefaultMultiUserAccess	1770
このポリシーを使用すると	1770
ポリシーの詳細	1770
ポリシーのバージョン	1770
JSON ポリシードキュメント	1770
詳細はこちら	1772
AWSDeepRacerFullAccess	1772
このポリシーを使用すると	1772
ポリシーの詳細	1772
ポリシーのバージョン	1773
JSON ポリシードキュメント	1773
詳細はこちら	1774

AWSDeepRacerRoboMakerAccessPolicy	1774
このポリシーを使用すると	1774
ポリシーの詳細	1774
ポリシーのバージョン	1774
JSON ポリシードキュメント	1775
詳細はこちら	1777
AWSDeepRacerServiceRolePolicy	1777
このポリシーを使用すると	1777
ポリシーの詳細	1777
ポリシーのバージョン	1777
JSON ポリシードキュメント	1777
詳細はこちら	1781
AWSDenyAll	1781
このポリシーを使用すると	1781
ポリシーの詳細	1781
ポリシーのバージョン	1781
JSON ポリシードキュメント	1781
詳細はこちら	1782
AWSDeviceFarmFullAccess	1782
このポリシーを使用すると	1782
ポリシーの詳細	1782
ポリシーのバージョン	1782
JSON ポリシードキュメント	1783
詳細はこちら	1783
AWSDeviceFarmServiceRolePolicy	1783
このポリシーを使用すると	1783
ポリシーの詳細	1784
ポリシーのバージョン	1784
JSON ポリシードキュメント	1784
詳細はこちら	1786
AWSDeviceFarmTestGridServiceRolePolicy	1786
このポリシーを使用すると	1786
ポリシーの詳細	1787
ポリシーのバージョン	1787
JSON ポリシードキュメント	1787
詳細はこちら	1789

AWSDirectConnectFullAccess	1789
このポリシーを使用すると	1789
ポリシーの詳細	1789
ポリシーのバージョン	1790
JSON ポリシードキュメント	1790
詳細はこちら	1790
AWSDirectConnectReadOnlyAccess	1791
このポリシーを使用すると	1791
ポリシーの詳細	1791
ポリシーのバージョン	1791
JSON ポリシードキュメント	1791
詳細はこちら	1792
AWSDirectConnectServiceRolePolicy	1792
このポリシーを使用すると	1792
ポリシーの詳細	1792
ポリシーのバージョン	1792
JSON ポリシードキュメント	1793
詳細はこちら	1793
AWSDirectoryServiceFullAccess	1793
このポリシーを使用すると	1793
ポリシーの詳細	1794
ポリシーのバージョン	1794
JSON ポリシードキュメント	1794
詳細はこちら	1796
AWSDirectoryServiceReadOnlyAccess	1796
このポリシーを使用すると	1796
ポリシーの詳細	1796
ポリシーのバージョン	1796
JSON ポリシードキュメント	1797
詳細はこちら	1797
AWSDiscoveryContinuousExportFirehosePolicy	1798
このポリシーを使用すると	1798
ポリシーの詳細	1798
ポリシーのバージョン	1798
JSON ポリシードキュメント	1798
詳細はこちら	1799

AWSDMSFleetAdvisorServiceRolePolicy	1799
このポリシーを使用すると	1800
ポリシーの詳細	1800
ポリシーのバージョン	1800
JSON ポリシードキュメント	1800
詳細はこちら	1801
AWSDMSServerlessServiceRolePolicy	1801
このポリシーを使用すると	1801
ポリシーの詳細	1801
ポリシーのバージョン	1801
JSON ポリシードキュメント	1801
詳細はこちら	1803
AWSEC2CapacityReservationFleetRolePolicy	1803
このポリシーを使用すると	1803
ポリシーの詳細	1803
ポリシーのバージョン	1804
JSON ポリシードキュメント	1804
詳細はこちら	1805
AWSEC2FleetServiceRolePolicy	1805
このポリシーを使用すると	1805
ポリシーの詳細	1805
ポリシーのバージョン	1806
JSON ポリシードキュメント	1806
詳細はこちら	1808
AWSEC2SpotFleetServiceRolePolicy	1808
このポリシーを使用すると	1808
ポリシーの詳細	1808
ポリシーのバージョン	1808
JSON ポリシードキュメント	1809
詳細はこちら	1811
AWSEC2SpotServiceRolePolicy	1811
このポリシーを使用すると	1811
ポリシーの詳細	1811
ポリシーのバージョン	1811
JSON ポリシードキュメント	1811
詳細はこちら	1813

AWSEC2VssSnapshotPolicy	1813
このポリシーを使用すると	1813
ポリシーの詳細	1813
ポリシーのバージョン	1814
JSON ポリシードキュメント	1814
詳細はこちら	1817
AWSECRPullThroughCache_ServiceRolePolicy	1817
このポリシーを使用すると	1817
ポリシーの詳細	1817
ポリシーのバージョン	1818
JSON ポリシードキュメント	1818
詳細はこちら	1819
AWSElasticBeanstalkCustomPlatformforEC2Role	1819
このポリシーを使用すると	1819
ポリシーの詳細	1819
ポリシーのバージョン	1819
JSON ポリシードキュメント	1820
詳細はこちら	1821
AWSElasticBeanstalkEnhancedHealth	1821
このポリシーを使用すると	1822
ポリシーの詳細	1822
ポリシーのバージョン	1822
JSON ポリシードキュメント	1822
詳細はこちら	1823
AWSElasticBeanstalkMaintenance	1823
このポリシーを使用すると	1824
ポリシーの詳細	1824
ポリシーのバージョン	1824
JSON ポリシードキュメント	1824
詳細はこちら	1825
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy	1825
このポリシーを使用すると	1825
ポリシーの詳細	1825
ポリシーのバージョン	1826
JSON ポリシードキュメント	1826
詳細はこちら	1833

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy	1833
このポリシーを使用すると	1833
ポリシーの詳細	1833
ポリシーのバージョン	1833
JSON ポリシードキュメント	1834
詳細はこちら	1839
AWSElasticBeanstalkMulticontainerDocker	1839
このポリシーを使用すると	1839
ポリシーの詳細	1839
ポリシーのバージョン	1840
JSON ポリシードキュメント	1840
詳細はこちら	1841
AWSElasticBeanstalkReadOnly	1841
このポリシーを使用すると	1841
ポリシーの詳細	1841
ポリシーのバージョン	1841
JSON ポリシードキュメント	1842
詳細はこちら	1844
AWSElasticBeanstalkRoleCore	1844
このポリシーを使用すると	1844
ポリシーの詳細	1844
ポリシーのバージョン	1844
JSON ポリシードキュメント	1845
詳細はこちら	1849
AWSElasticBeanstalkRoleCWL	1850
このポリシーを使用すると	1850
ポリシーの詳細	1850
ポリシーのバージョン	1850
JSON ポリシードキュメント	1850
詳細はこちら	1851
AWSElasticBeanstalkRoleECS	1851
このポリシーを使用すると	1851
ポリシーの詳細	1851
ポリシーのバージョン	1851
JSON ポリシードキュメント	1852
詳細はこちら	1853

AWSElasticBeanstalkRoleRDS	1853
このポリシーを使用すると	1853
ポリシーの詳細	1853
ポリシーのバージョン	1853
JSON ポリシードキュメント	1853
詳細はこちら	1854
AWSElasticBeanstalkRoleSNS	1854
このポリシーを使用すると	1854
ポリシーの詳細	1855
ポリシーのバージョン	1855
JSON ポリシードキュメント	1855
詳細はこちら	1856
AWSElasticBeanstalkRoleWorkerTier	1856
このポリシーを使用すると	1856
ポリシーの詳細	1856
ポリシーのバージョン	1856
JSON ポリシードキュメント	1857
詳細はこちら	1857
AWSElasticBeanstalkService	1858
このポリシーを使用すると	1858
ポリシーの詳細	1858
ポリシーのバージョン	1858
JSON ポリシードキュメント	1858
詳細はこちら	1863
AWSElasticBeanstalkServiceRolePolicy	1863
このポリシーを使用すると	1863
ポリシーの詳細	1863
ポリシーのバージョン	1863
JSON ポリシードキュメント	1864
詳細はこちら	1865
AWSElasticBeanstalkWebTier	1865
このポリシーを使用すると	1865
ポリシーの詳細	1865
ポリシーのバージョン	1866
JSON ポリシードキュメント	1866
詳細はこちら	1867

AWSElasticBeanstalkWorkerTier	1867
このポリシーを使用すると	1868
ポリシーの詳細	1868
ポリシーのバージョン	1868
JSON ポリシードキュメント	1868
詳細はこちら	1870
AWSElasticDisasterRecoveryAgentInstallationPolicy	1870
このポリシーを使用すると	1871
ポリシーの詳細	1871
ポリシーのバージョン	1871
JSON ポリシードキュメント	1871
詳細はこちら	1873
AWSElasticDisasterRecoveryAgentPolicy	1873
このポリシーを使用すると	1873
ポリシーの詳細	1873
ポリシーのバージョン	1873
JSON ポリシードキュメント	1874
詳細はこちら	1874
AWSElasticDisasterRecoveryConsoleFullAccess	1875
このポリシーを使用すると	1875
ポリシーの詳細	1875
ポリシーのバージョン	1875
JSON ポリシードキュメント	1875
詳細はこちら	1885
AWSElasticDisasterRecoveryConsoleFullAccess_v2	1885
このポリシーを使用すると	1885
ポリシーの詳細	1886
ポリシーのバージョン	1886
JSON ポリシードキュメント	1886
詳細はこちら	1899
AWSElasticDisasterRecoveryConversionServerPolicy	1899
このポリシーを使用すると	1899
ポリシーの詳細	1899
ポリシーのバージョン	1900
JSON ポリシードキュメント	1900
詳細はこちら	1900

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy	1901
このポリシーを使用すると	1901
ポリシーの詳細	1901
ポリシーのバージョン	1901
JSON ポリシードキュメント	1901
詳細はこちら	1902
AWSElasticDisasterRecoveryEc2InstancePolicy	1902
このポリシーを使用すると	1903
ポリシーの詳細	1903
ポリシーのバージョン	1903
JSON ポリシードキュメント	1903
詳細はこちら	1905
AWSElasticDisasterRecoveryFailbackInstallationPolicy	1905
このポリシーを使用すると	1906
ポリシーの詳細	1906
ポリシーのバージョン	1906
JSON ポリシードキュメント	1906
詳細はこちら	1907
AWSElasticDisasterRecoveryFailbackPolicy	1907
このポリシーを使用すると	1907
ポリシーの詳細	1907
ポリシーのバージョン	1908
JSON ポリシードキュメント	1908
詳細はこちら	1909
AWSElasticDisasterRecoveryLaunchActionsPolicy	1909
このポリシーを使用すると	1909
ポリシーの詳細	1910
ポリシーのバージョン	1910
JSON ポリシードキュメント	1910
詳細はこちら	1916
AWSElasticDisasterRecoveryNetworkReplicationPolicy	1916
このポリシーを使用すると	1916
ポリシーの詳細	1916
ポリシーのバージョン	1917
JSON ポリシードキュメント	1917
詳細はこちら	1918

AWSElasticDisasterRecoveryReadOnlyAccess	1918
このポリシーを使用すると	1918
ポリシーの詳細	1918
ポリシーのバージョン	1918
JSON ポリシードキュメント	1919
詳細はこちら	1921
AWSElasticDisasterRecoveryRecoveryInstancePolicy	1921
このポリシーを使用すると	1921
ポリシーの詳細	1921
ポリシーのバージョン	1922
JSON ポリシードキュメント	1922
詳細はこちら	1924
AWSElasticDisasterRecoveryReplicationServerPolicy	1924
このポリシーを使用すると	1925
ポリシーの詳細	1925
ポリシーのバージョン	1925
JSON ポリシードキュメント	1925
詳細はこちら	1927
AWSElasticDisasterRecoveryServiceRolePolicy	1928
このポリシーを使用すると	1928
ポリシーの詳細	1928
ポリシーのバージョン	1928
JSON ポリシードキュメント	1928
詳細はこちら	1937
AWSElasticDisasterRecoveryStagingAccountPolicy	1937
このポリシーを使用すると	1937
ポリシーの詳細	1937
ポリシーのバージョン	1938
JSON ポリシードキュメント	1938
詳細はこちら	1939
AWSElasticDisasterRecoveryStagingAccountPolicy_v2	1939
このポリシーを使用すると	1939
ポリシーの詳細	1939
ポリシーのバージョン	1939
JSON ポリシードキュメント	1940
詳細はこちら	1941

AWSElasticLoadBalancingClassicServiceRolePolicy	1941
このポリシーを使用すると	1941
ポリシーの詳細	1941
ポリシーのバージョン	1941
JSON ポリシードキュメント	1942
詳細はこちら	1942
AWSElasticLoadBalancingServiceRolePolicy	1943
このポリシーを使用すると	1943
ポリシーの詳細	1943
ポリシーのバージョン	1943
JSON ポリシードキュメント	1943
詳細はこちら	1944
AWSElementalMediaConvertFullAccess	1945
このポリシーを使用すると	1945
ポリシーの詳細	1945
ポリシーのバージョン	1945
JSON ポリシードキュメント	1945
詳細はこちら	1946
AWSElementalMediaConvertReadOnly	1946
このポリシーを使用すると	1946
ポリシーの詳細	1947
ポリシーのバージョン	1947
JSON ポリシードキュメント	1947
詳細はこちら	1947
AWSElementalMediaLiveFullAccess	1948
このポリシーを使用すると	1948
ポリシーの詳細	1948
ポリシーのバージョン	1948
JSON ポリシードキュメント	1948
詳細はこちら	1949
AWSElementalMediaLiveReadOnly	1949
このポリシーを使用すると	1949
ポリシーの詳細	1949
ポリシーのバージョン	1949
JSON ポリシードキュメント	1949
詳細はこちら	1950

AWSElementalMediaPackageFullAccess	1950
このポリシーを使用すると	1950
ポリシーの詳細	1950
ポリシーのバージョン	1950
JSON ポリシードキュメント	1951
詳細はこちら	1951
AWSElementalMediaPackageReadOnly	1951
このポリシーを使用すると	1951
ポリシーの詳細	1951
ポリシーのバージョン	1952
JSON ポリシードキュメント	1952
詳細はこちら	1952
AWSElementalMediaPackageV2FullAccess	1952
このポリシーを使用すると	1953
ポリシーの詳細	1953
ポリシーのバージョン	1953
JSON ポリシードキュメント	1953
詳細はこちら	1953
AWSElementalMediaPackageV2ReadOnly	1954
このポリシーを使用すると	1954
ポリシーの詳細	1954
ポリシーのバージョン	1954
JSON ポリシードキュメント	1954
詳細はこちら	1955
AWSElementalMediaStoreFullAccess	1955
このポリシーを使用すると	1955
ポリシーの詳細	1955
ポリシーのバージョン	1955
JSON ポリシードキュメント	1955
詳細はこちら	1956
AWSElementalMediaStoreReadOnly	1956
このポリシーを使用すると	1956
ポリシーの詳細	1956
ポリシーのバージョン	1957
JSON ポリシードキュメント	1957
詳細はこちら	1957

AWSElementalMediaTailorFullAccess	1957
このポリシーを使用すると	1958
ポリシーの詳細	1958
ポリシーのバージョン	1958
JSON ポリシードキュメント	1958
詳細はこちら	1958
AWSElementalMediaTailorReadOnly	1959
このポリシーを使用すると	1959
ポリシーの詳細	1959
ポリシーのバージョン	1959
JSON ポリシードキュメント	1959
詳細はこちら	1960
AWSEnhancedClassicNetworkingMangementPolicy	1960
このポリシーを使用すると	1960
ポリシーの詳細	1960
ポリシーのバージョン	1960
JSON ポリシードキュメント	1961
詳細はこちら	1961
AWSEntityResolutionConsoleFullAccess	1961
このポリシーを使用すると	1961
ポリシーの詳細	1961
ポリシーのバージョン	1962
JSON ポリシードキュメント	1962
詳細はこちら	1964
AWSEntityResolutionConsoleReadOnlyAccess	1965
このポリシーを使用すると	1965
ポリシーの詳細	1965
ポリシーのバージョン	1965
JSON ポリシードキュメント	1965
詳細はこちら	1966
AWSFaultInjectionSimulatorEC2Access	1966
このポリシーを使用すると	1966
ポリシーの詳細	1966
ポリシーのバージョン	1967
JSON ポリシードキュメント	1967
詳細はこちら	1968

AWSFaultInjectionSimulatorECSAccess	1968
このポリシーを使用すると	1969
ポリシーの詳細	1969
ポリシーのバージョン	1969
JSON ポリシードキュメント	1969
詳細はこちら	1971
AWSFaultInjectionSimulatorEKSAccess	1971
このポリシーを使用すると	1971
ポリシーの詳細	1971
ポリシーのバージョン	1972
JSON ポリシードキュメント	1972
詳細はこちら	1973
AWSFaultInjectionSimulatorNetworkAccess	1973
このポリシーを使用すると	1973
ポリシーの詳細	1973
ポリシーのバージョン	1974
JSON ポリシードキュメント	1974
詳細はこちら	1981
AWSFaultInjectionSimulatorRDSAccess	1981
このポリシーを使用すると	1981
ポリシーの詳細	1981
ポリシーのバージョン	1981
JSON ポリシードキュメント	1982
詳細はこちら	1983
AWSFaultInjectionSimulatorSSMAccess	1983
このポリシーを使用すると	1983
ポリシーの詳細	1983
ポリシーのバージョン	1983
JSON ポリシードキュメント	1984
詳細はこちら	1985
AWSFinSpaceServiceRolePolicy	1985
このポリシーを使用すると	1985
ポリシーの詳細	1985
ポリシーのバージョン	1986
JSON ポリシードキュメント	1986
詳細はこちら	1986

AWSFMAdminFullAccess	1987
このポリシーを使用すると	1987
ポリシーの詳細	1987
ポリシーのバージョン	1987
JSON ポリシードキュメント	1987
詳細はこちら	1989
AWSFMAdminReadOnlyAccess	1989
このポリシーを使用すると	1989
ポリシーの詳細	1989
ポリシーのバージョン	1990
JSON ポリシードキュメント	1990
詳細はこちら	1991
AWSFMMemberReadOnlyAccess	1992
このポリシーを使用すると	1992
ポリシーの詳細	1992
ポリシーのバージョン	1992
JSON ポリシードキュメント	1992
詳細はこちら	1993
AWSForWordPressPluginPolicy	1993
このポリシーを使用すると	1993
ポリシーの詳細	1993
ポリシーのバージョン	1993
JSON ポリシードキュメント	1994
詳細はこちら	1995
AWSGitSyncServiceRolePolicy	1996
このポリシーを使用すると	1996
ポリシーの詳細	1996
ポリシーのバージョン	1996
JSON ポリシードキュメント	1996
詳細はこちら	1997
AWSGlobalAcceleratorSLRPolicy	1997
このポリシーを使用すると	1997
ポリシーの詳細	1997
ポリシーのバージョン	1998
JSON ポリシードキュメント	1998
詳細はこちら	1999

AWSGlueConsoleFullAccess	1999
このポリシーを使用すると	2000
ポリシーの詳細	2000
ポリシーのバージョン	2000
JSON ポリシードキュメント	2000
詳細はこちら	2004
AWSGlueConsoleSageMakerNotebookFullAccess	2004
このポリシーを使用すると	2005
ポリシーの詳細	2005
ポリシーのバージョン	2005
JSON ポリシードキュメント	2005
詳細はこちら	2010
AwsGlueDataBrewFullAccessPolicy	2010
このポリシーを使用すると	2011
ポリシーの詳細	2011
ポリシーのバージョン	2011
JSON ポリシードキュメント	2011
詳細はこちら	2016
AWSGlueDataBrewServiceRole	2016
このポリシーを使用すると	2017
ポリシーの詳細	2017
ポリシーのバージョン	2017
JSON ポリシードキュメント	2017
詳細はこちら	2020
AWSGlueSchemaRegistryFullAccess	2020
このポリシーを使用すると	2020
ポリシーの詳細	2020
ポリシーのバージョン	2021
JSON ポリシードキュメント	2021
詳細はこちら	2022
AWSGlueSchemaRegistryReadOnlyAccess	2022
このポリシーを使用すると	2022
ポリシーの詳細	2022
ポリシーのバージョン	2023
JSON ポリシードキュメント	2023
詳細はこちら	2024

AWSGlueServiceNotebookRole	2024
このポリシーを使用すると	2024
ポリシーの詳細	2024
ポリシーのバージョン	2024
JSON ポリシードキュメント	2024
詳細はこちら	2027
AWSGlueServiceRole	2027
このポリシーを使用すると	2027
ポリシーの詳細	2027
ポリシーのバージョン	2027
JSON ポリシードキュメント	2028
詳細はこちら	2030
AwsGlueSessionUserRestrictedNotebookPolicy	2030
このポリシーを使用すると	2030
ポリシーの詳細	2030
ポリシーのバージョン	2031
JSON ポリシードキュメント	2031
詳細はこちら	2033
AwsGlueSessionUserRestrictedNotebookServiceRole	2033
このポリシーを使用すると	2034
ポリシーの詳細	2034
ポリシーのバージョン	2034
JSON ポリシードキュメント	2034
詳細はこちら	2038
AwsGlueSessionUserRestrictedPolicy	2038
このポリシーを使用すると	2038
ポリシーの詳細	2038
ポリシーのバージョン	2039
JSON ポリシードキュメント	2039
詳細はこちら	2041
AwsGlueSessionUserRestrictedServiceRole	2041
このポリシーを使用すると	2042
ポリシーの詳細	2042
ポリシーのバージョン	2042
JSON ポリシードキュメント	2042
詳細はこちら	2046

AWSGrafanaAccountAdministrator	2047
このポリシーを使用すると	2047
ポリシーの詳細	2047
ポリシーのバージョン	2047
JSON ポリシードキュメント	2047
詳細はこちら	2048
AWSGrafanaConsoleReadOnlyAccess	2048
このポリシーを使用すると	2049
ポリシーの詳細	2049
ポリシーのバージョン	2049
JSON ポリシードキュメント	2049
詳細はこちら	2050
AWSGrafanaWorkspacePermissionManagement	2050
このポリシーを使用すると	2050
ポリシーの詳細	2050
ポリシーのバージョン	2050
JSON ポリシードキュメント	2050
詳細はこちら	2051
AWSGrafanaWorkspacePermissionManagementV2	2052
このポリシーを使用すると	2052
ポリシーの詳細	2052
ポリシーのバージョン	2052
JSON ポリシードキュメント	2052
詳細はこちら	2053
AWSGreengrassFullAccess	2053
このポリシーを使用すると	2053
ポリシーの詳細	2054
ポリシーのバージョン	2054
JSON ポリシードキュメント	2054
詳細はこちら	2054
AWSGreengrassReadOnlyAccess	2055
このポリシーを使用すると	2055
ポリシーの詳細	2055
ポリシーのバージョン	2055
JSON ポリシードキュメント	2055
詳細はこちら	2056

AWSGreengrassResourceAccessRolePolicy	2056
このポリシーを使用すると	2056
ポリシーの詳細	2056
ポリシーのバージョン	2056
JSON ポリシードキュメント	2057
詳細はこちら	2059
AWSGroundStationAgentInstancePolicy	2059
このポリシーを使用すると	2059
ポリシーの詳細	2059
ポリシーのバージョン	2060
JSON ポリシードキュメント	2060
詳細はこちら	2060
AWSHealth_EventProcessorServiceRolePolicy	2060
このポリシーを使用すると	2061
ポリシーの詳細	2061
ポリシーのバージョン	2061
JSON ポリシードキュメント	2061
詳細はこちら	2062
AWSHealthFullAccess	2062
このポリシーを使用すると	2062
ポリシーの詳細	2062
ポリシーのバージョン	2062
JSON ポリシードキュメント	2063
詳細はこちら	2064
AWSHealthImagingFullAccess	2064
このポリシーを使用すると	2064
ポリシーの詳細	2064
ポリシーのバージョン	2064
JSON ポリシードキュメント	2065
詳細はこちら	2065
AWSHealthImagingReadOnlyAccess	2065
このポリシーを使用すると	2066
ポリシーの詳細	2066
ポリシーのバージョン	2066
JSON ポリシードキュメント	2066
詳細はこちら	2067

AWSIAMIdentityCenterAllowListForIdentityContext	2067
このポリシーを使用すると	2067
ポリシーの詳細	2067
ポリシーのバージョン	2067
JSON ポリシードキュメント	2068
詳細はこちら	2070
AWSIdentitySyncFullAccess	2071
このポリシーを使用すると	2071
ポリシーの詳細	2071
ポリシーのバージョン	2071
JSON ポリシードキュメント	2071
詳細はこちら	2072
AWSIdentitySyncReadOnlyAccess	2072
このポリシーを使用すると	2072
ポリシーの詳細	2072
ポリシーのバージョン	2073
JSON ポリシードキュメント	2073
詳細はこちら	2073
AWSImageBuilderFullAccess	2074
このポリシーを使用すると	2074
ポリシーの詳細	2074
ポリシーのバージョン	2074
JSON ポリシードキュメント	2074
詳細はこちら	2077
AWSImageBuilderReadOnlyAccess	2077
このポリシーを使用すると	2077
ポリシーの詳細	2077
ポリシーのバージョン	2078
JSON ポリシードキュメント	2078
詳細はこちら	2078
AWSImportExportFullAccess	2079
このポリシーを使用すると	2079
ポリシーの詳細	2079
ポリシーのバージョン	2079
JSON ポリシードキュメント	2079
詳細はこちら	2080

AWSImportExportReadOnlyAccess	2080
このポリシーを使用すると	2080
ポリシーの詳細	2080
ポリシーのバージョン	2080
JSON ポリシードキュメント	2080
詳細はこちら	2081
AWSIncidentManagerIncidentAccessServiceRolePolicy	2081
このポリシーを使用すると	2081
ポリシーの詳細	2081
ポリシーのバージョン	2082
JSON ポリシードキュメント	2082
詳細はこちら	2082
AWSIncidentManagerResolverAccess	2083
このポリシーを使用すると	2083
ポリシーの詳細	2083
ポリシーのバージョン	2083
JSON ポリシードキュメント	2083
詳細はこちら	2084
AWSIncidentManagerServiceRolePolicy	2085
このポリシーを使用すると	2085
ポリシーの詳細	2085
ポリシーのバージョン	2085
JSON ポリシードキュメント	2085
詳細はこちら	2086
AWSIoT1ClickFullAccess	2087
このポリシーを使用すると	2087
ポリシーの詳細	2087
ポリシーのバージョン	2087
JSON ポリシードキュメント	2087
詳細はこちら	2088
AWSIoT1ClickReadOnlyAccess	2088
このポリシーを使用すると	2088
ポリシーの詳細	2088
ポリシーのバージョン	2088
JSON ポリシードキュメント	2088
詳細はこちら	2089

AWSIoTAnalyticsFullAccess	2089
このポリシーを使用すると	2089
ポリシーの詳細	2089
ポリシーのバージョン	2090
JSON ポリシードキュメント	2090
詳細はこちら	2090
AWSIoTAnalyticsReadOnlyAccess	2090
このポリシーを使用すると	2090
ポリシーの詳細	2091
ポリシーのバージョン	2091
JSON ポリシードキュメント	2091
詳細はこちら	2091
AWSIoTConfigAccess	2092
このポリシーを使用すると	2092
ポリシーの詳細	2092
ポリシーのバージョン	2092
JSON ポリシードキュメント	2092
詳細はこちら	2096
AWSIoTConfigReadOnlyAccess	2096
このポリシーを使用すると	2096
ポリシーの詳細	2097
ポリシーのバージョン	2097
JSON ポリシードキュメント	2097
詳細はこちら	2099
AWSIoTDataAccess	2099
このポリシーを使用すると	2099
ポリシーの詳細	2099
ポリシーのバージョン	2100
JSON ポリシードキュメント	2100
詳細はこちら	2100
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction	2101
このポリシーを使用すると	2101
ポリシーの詳細	2101
ポリシーのバージョン	2101
JSON ポリシードキュメント	2101
詳細はこちら	2102

AWSIoTDeviceDefenderAudit	2102
このポリシーを使用すると	2102
ポリシーの詳細	2102
ポリシーのバージョン	2102
JSON ポリシードキュメント	2103
詳細はこちら	2104
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction	2104
このポリシーを使用すると	2104
ポリシーの詳細	2104
ポリシーのバージョン	2104
JSON ポリシードキュメント	2105
詳細はこちら	2105
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction	2106
このポリシーを使用すると	2106
ポリシーの詳細	2106
ポリシーのバージョン	2106
JSON ポリシードキュメント	2106
詳細はこちら	2107
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction	2107
このポリシーを使用すると	2107
ポリシーの詳細	2107
ポリシーのバージョン	2108
JSON ポリシードキュメント	2108
詳細はこちら	2108
AWSIoTDeviceDefenderUpdateCACertMitigationAction	2108
このポリシーを使用すると	2109
ポリシーの詳細	2109
ポリシーのバージョン	2109
JSON ポリシードキュメント	2109
詳細はこちら	2110
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction	2110
このポリシーを使用すると	2110
ポリシーの詳細	2110
ポリシーのバージョン	2110
JSON ポリシードキュメント	2111
詳細はこちら	2111

AWSIoTDeviceTesterForFreeRTOSFullAccess	2111
このポリシーを使用すると	2111
ポリシーの詳細	2111
ポリシーのバージョン	2112
JSON ポリシードキュメント	2112
詳細はこちら	2118
AWSIoTDeviceTesterForGreengrassFullAccess	2118
このポリシーを使用すると	2118
ポリシーの詳細	2118
ポリシーのバージョン	2119
JSON ポリシードキュメント	2119
詳細はこちら	2122
AWSIoTEventsFullAccess	2122
このポリシーを使用すると	2122
ポリシーの詳細	2122
ポリシーのバージョン	2122
JSON ポリシードキュメント	2123
詳細はこちら	2123
AWSIoTEventsReadOnlyAccess	2123
このポリシーを使用すると	2123
ポリシーの詳細	2123
ポリシーのバージョン	2124
JSON ポリシードキュメント	2124
詳細はこちら	2124
AWSIoTFleetHubFederationAccess	2124
このポリシーを使用すると	2124
ポリシーの詳細	2125
ポリシーのバージョン	2125
JSON ポリシードキュメント	2125
詳細はこちら	2127
AWSIoTFleetwiseServiceRolePolicy	2127
このポリシーを使用すると	2127
ポリシーの詳細	2127
ポリシーのバージョン	2127
JSON ポリシードキュメント	2128
詳細はこちら	2128

AWSIoTFullAccess	2128
このポリシーを使用すると	2129
ポリシーの詳細	2129
ポリシーのバージョン	2129
JSON ポリシードキュメント	2129
詳細はこちら	2129
AWSIoTLogging	2130
このポリシーを使用すると	2130
ポリシーの詳細	2130
ポリシーのバージョン	2130
JSON ポリシードキュメント	2130
詳細はこちら	2131
AWSIoTOTAUpdate	2131
このポリシーを使用すると	2131
ポリシーの詳細	2131
ポリシーのバージョン	2132
JSON ポリシードキュメント	2132
詳細はこちら	2132
AWSIoTRoboRunnerFullAccess	2132
このポリシーを使用すると	2133
ポリシーの詳細	2133
ポリシーのバージョン	2133
JSON ポリシードキュメント	2133
詳細はこちら	2134
AWSIoTRoboRunnerReadOnly	2134
このポリシーを使用すると	2134
ポリシーの詳細	2134
ポリシーのバージョン	2134
JSON ポリシードキュメント	2135
詳細はこちら	2135
AWSIoTRoboRunnerServiceRolePolicy	2135
このポリシーを使用すると	2136
ポリシーの詳細	2136
ポリシーのバージョン	2136
JSON ポリシードキュメント	2136
詳細はこちら	2137

AWSIoTRuleActions	2137
このポリシーを使用すると	2137
ポリシーの詳細	2137
ポリシーのバージョン	2137
JSON ポリシードキュメント	2137
詳細はこちら	2138
AWSIoTSiteWiseConsoleFullAccess	2138
このポリシーを使用すると	2138
ポリシーの詳細	2139
ポリシーのバージョン	2139
JSON ポリシードキュメント	2139
詳細はこちら	2141
AWSIoTSiteWiseFullAccess	2141
このポリシーを使用すると	2141
ポリシーの詳細	2141
ポリシーのバージョン	2142
JSON ポリシードキュメント	2142
詳細はこちら	2142
AWSIoTSiteWiseMonitorPortalAccess	2142
このポリシーを使用すると	2143
ポリシーの詳細	2143
ポリシーのバージョン	2143
JSON ポリシードキュメント	2143
詳細はこちら	2144
AWSIoTSiteWiseMonitorServiceRolePolicy	2144
このポリシーを使用すると	2145
ポリシーの詳細	2145
ポリシーのバージョン	2145
JSON ポリシードキュメント	2145
詳細はこちら	2146
AWSIoTSiteWiseReadOnlyAccess	2146
このポリシーを使用すると	2146
ポリシーの詳細	2146
ポリシーのバージョン	2147
JSON ポリシードキュメント	2147
詳細はこちら	2147

AWSIoTThingsRegistration	2148
このポリシーを使用すると	2148
ポリシーの詳細	2148
ポリシーのバージョン	2148
JSON ポリシードキュメント	2148
詳細はこちら	2149
AWSIoTtwinMakerServiceRolePolicy	2150
このポリシーを使用すると	2150
ポリシーの詳細	2150
ポリシーのバージョン	2150
JSON ポリシードキュメント	2150
詳細はこちら	2152
AWSIoTWirelessDataAccess	2152
このポリシーを使用すると	2152
ポリシーの詳細	2152
ポリシーのバージョン	2152
JSON ポリシードキュメント	2153
詳細はこちら	2153
AWSIoTWirelessFullAccess	2153
このポリシーを使用すると	2153
ポリシーの詳細	2154
ポリシーのバージョン	2154
JSON ポリシードキュメント	2154
詳細はこちら	2154
AWSIoTWirelessFullPublishAccess	2155
このポリシーを使用すると	2155
ポリシーの詳細	2155
ポリシーのバージョン	2155
JSON ポリシードキュメント	2155
詳細はこちら	2156
AWSIoTWirelessGatewayCertManager	2156
このポリシーを使用すると	2156
ポリシーの詳細	2156
ポリシーのバージョン	2156
JSON ポリシードキュメント	2157
詳細はこちら	2157

AWSIoTWirelessLogging	2157
このポリシーを使用すると	2157
ポリシーの詳細	2158
ポリシーのバージョン	2158
JSON ポリシードキュメント	2158
詳細はこちら	2158
AWSIoTWirelessReadOnlyAccess	2159
このポリシーを使用すると	2159
ポリシーの詳細	2159
ポリシーのバージョン	2159
JSON ポリシードキュメント	2159
詳細はこちら	2160
AWSIPAMServiceRolePolicy	2160
このポリシーを使用すると	2160
ポリシーの詳細	2160
ポリシーのバージョン	2160
JSON ポリシードキュメント	2161
詳細はこちら	2162
AWSIQContractServiceRolePolicy	2162
このポリシーを使用すると	2162
ポリシーの詳細	2162
ポリシーのバージョン	2162
JSON ポリシードキュメント	2163
詳細はこちら	2163
AWSIQFullAccess	2163
このポリシーを使用すると	2163
ポリシーの詳細	2163
ポリシーのバージョン	2164
JSON ポリシードキュメント	2164
詳細はこちら	2165
AWSIQPermissionServiceRolePolicy	2165
このポリシーを使用すると	2165
ポリシーの詳細	2165
ポリシーのバージョン	2165
JSON ポリシードキュメント	2166
詳細はこちら	2166

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy	2167
このポリシーを使用すると	2167
ポリシーの詳細	2167
ポリシーのバージョン	2167
JSON ポリシードキュメント	2167
詳細はこちら	2168
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy	2168
このポリシーを使用すると	2168
ポリシーの詳細	2168
ポリシーのバージョン	2169
JSON ポリシードキュメント	2169
詳細はこちら	2169
AWSKeyManagementServicePowerUser	2169
このポリシーを使用すると	2169
ポリシーの詳細	2170
ポリシーのバージョン	2170
JSON ポリシードキュメント	2170
詳細はこちら	2171
AWSLakeFormationCrossAccountManager	2171
このポリシーを使用すると	2171
ポリシーの詳細	2171
ポリシーのバージョン	2171
JSON ポリシードキュメント	2171
詳細はこちら	2173
AWSLakeFormationDataAdmin	2174
このポリシーを使用すると	2174
ポリシーの詳細	2174
ポリシーのバージョン	2174
JSON ポリシードキュメント	2174
詳細はこちら	2175
AWSLambda_FullAccess	2176
このポリシーを使用すると	2176
ポリシーの詳細	2176
ポリシーのバージョン	2176
JSON ポリシードキュメント	2176
詳細はこちら	2178

AWSLambda_ReadOnlyAccess	2178
このポリシーを使用すると	2178
ポリシーの詳細	2178
ポリシーのバージョン	2178
JSON ポリシードキュメント	2179
詳細はこちら	2180
AWSLambdaBasicExecutionRole	2180
このポリシーを使用すると	2180
ポリシーの詳細	2180
ポリシーのバージョン	2180
JSON ポリシードキュメント	2181
詳細はこちら	2181
AWSLambdaDynamoDBExecutionRole	2181
このポリシーを使用すると	2181
ポリシーの詳細	2182
ポリシーのバージョン	2182
JSON ポリシードキュメント	2182
詳細はこちら	2182
AWSLambdaENIManagementAccess	2183
このポリシーを使用すると	2183
ポリシーの詳細	2183
ポリシーのバージョン	2183
JSON ポリシードキュメント	2183
詳細はこちら	2184
AWSLambdaExecute	2184
このポリシーを使用すると	2184
ポリシーの詳細	2184
ポリシーのバージョン	2184
JSON ポリシードキュメント	2185
詳細はこちら	2185
AWSLambdaFullAccess	2185
このポリシーを使用すると	2186
ポリシーの詳細	2186
ポリシーのバージョン	2186
JSON ポリシードキュメント	2186
詳細はこちら	2188

AWSLambdaInvocation-DynamoDB	2188
このポリシーを使用すると	2188
ポリシーの詳細	2188
ポリシーのバージョン	2188
JSON ポリシードキュメント	2189
詳細はこちら	2189
AWSLambdaKinesisExecutionRole	2189
このポリシーを使用すると	2190
ポリシーの詳細	2190
ポリシーのバージョン	2190
JSON ポリシードキュメント	2190
詳細はこちら	2191
AWSLambdaMSKExecutionRole	2191
このポリシーを使用すると	2191
ポリシーの詳細	2191
ポリシーのバージョン	2191
JSON ポリシードキュメント	2192
詳細はこちら	2192
AWSLambdaReplicator	2192
このポリシーを使用すると	2193
ポリシーの詳細	2193
ポリシーのバージョン	2193
JSON ポリシードキュメント	2193
詳細はこちら	2194
AWSLambdaRole	2194
このポリシーを使用すると	2194
ポリシーの詳細	2195
ポリシーのバージョン	2195
JSON ポリシードキュメント	2195
詳細はこちら	2195
AWSLambdaSQSQueueExecutionRole	2196
このポリシーを使用すると	2196
ポリシーの詳細	2196
ポリシーのバージョン	2196
JSON ポリシードキュメント	2196
詳細はこちら	2197

AWSLambdaVPCAccessExecutionRole	2197
このポリシーを使用すると	2197
ポリシーの詳細	2197
ポリシーのバージョン	2197
JSON ポリシードキュメント	2198
詳細はこちら	2198
AWSLicenseManagerConsumptionPolicy	2198
このポリシーを使用すると	2199
ポリシーの詳細	2199
ポリシーのバージョン	2199
JSON ポリシードキュメント	2199
詳細はこちら	2200
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	2200
このポリシーを使用すると	2200
ポリシーの詳細	2200
ポリシーのバージョン	2200
JSON ポリシードキュメント	2201
詳細はこちら	2201
AWSLicenseManagerMasterAccountRolePolicy	2202
このポリシーを使用すると	2202
ポリシーの詳細	2202
ポリシーのバージョン	2202
JSON ポリシードキュメント	2202
詳細はこちら	2207
AWSLicenseManagerMemberAccountRolePolicy	2207
このポリシーを使用すると	2207
ポリシーの詳細	2208
ポリシーのバージョン	2208
JSON ポリシードキュメント	2208
詳細はこちら	2209
AWSLicenseManagerServiceRolePolicy	2209
このポリシーを使用すると	2209
ポリシーの詳細	2210
ポリシーのバージョン	2210
JSON ポリシードキュメント	2210
詳細はこちら	2213

AWSLicenseManagerUserSubscriptionsServiceRolePolicy	2213
このポリシーを使用すると	2214
ポリシーの詳細	2214
ポリシーのバージョン	2214
JSON ポリシードキュメント	2214
詳細はこちら	2216
AWSM2ServicePolicy	2216
このポリシーを使用すると	2216
ポリシーの詳細	2216
ポリシーのバージョン	2217
JSON ポリシードキュメント	2217
詳細はこちら	2218
AWSManagedServices_ContactsServiceRolePolicy	2218
このポリシーを使用すると	2219
ポリシーの詳細	2219
ポリシーのバージョン	2219
JSON ポリシードキュメント	2219
詳細はこちら	2220
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy	2220
このポリシーを使用すると	2220
ポリシーの詳細	2220
ポリシーのバージョン	2221
JSON ポリシードキュメント	2221
詳細はこちら	2222
AWSManagedServices_EventsServiceRolePolicy	2222
このポリシーを使用すると	2223
ポリシーの詳細	2223
ポリシーのバージョン	2223
JSON ポリシードキュメント	2223
詳細はこちら	2224
AWSManagedServicesDeploymentToolkitPolicy	2224
このポリシーを使用すると	2224
ポリシーの詳細	2224
ポリシーのバージョン	2225
JSON ポリシードキュメント	2225
詳細はこちら	2227

AWSMarketplaceAmiIngestion	2227
このポリシーを使用すると	2227
ポリシーの詳細	2227
ポリシーのバージョン	2227
JSON ポリシードキュメント	2228
詳細はこちら	2228
AWSMarketplaceDeploymentServiceRolePolicy	2229
このポリシーを使用すると	2229
ポリシーの詳細	2229
ポリシーのバージョン	2229
JSON ポリシードキュメント	2229
詳細はこちら	2231
AWSMarketplaceFullAccess	2231
このポリシーを使用すると	2231
ポリシーの詳細	2231
ポリシーのバージョン	2231
JSON ポリシードキュメント	2232
詳細はこちら	2235
AWSMarketplaceGetEntitlements	2235
このポリシーを使用すると	2235
ポリシーの詳細	2235
ポリシーのバージョン	2235
JSON ポリシードキュメント	2236
詳細はこちら	2236
AWSMarketplaceImageBuildFullAccess	2236
このポリシーを使用すると	2236
ポリシーの詳細	2236
ポリシーのバージョン	2237
JSON ポリシードキュメント	2237
詳細はこちら	2240
AWSMarketplaceLicenseManagementServiceRolePolicy	2241
このポリシーを使用すると	2241
ポリシーの詳細	2241
ポリシーのバージョン	2241
JSON ポリシードキュメント	2241
詳細はこちら	2242

AWSMarketplaceManageSubscriptions	2242
このポリシーを使用すると	2242
ポリシーの詳細	2242
ポリシーのバージョン	2243
JSON ポリシードキュメント	2243
詳細はこちら	2244
AWSMarketplaceMeteringFullAccess	2244
このポリシーを使用すると	2244
ポリシーの詳細	2244
ポリシーのバージョン	2244
JSON ポリシードキュメント	2245
詳細はこちら	2245
AWSMarketplaceMeteringRegisterUsage	2245
このポリシーを使用すると	2245
ポリシーの詳細	2245
ポリシーのバージョン	2246
JSON ポリシードキュメント	2246
詳細はこちら	2246
AWSMarketplaceProcurementSystemAdminFullAccess	2246
このポリシーを使用すると	2247
ポリシーの詳細	2247
ポリシーのバージョン	2247
JSON ポリシードキュメント	2247
詳細はこちら	2248
AWSMarketplacePurchaseOrdersServiceRolePolicy	2248
このポリシーを使用すると	2248
ポリシーの詳細	2248
ポリシーのバージョン	2248
JSON ポリシードキュメント	2249
詳細はこちら	2249
AWSMarketplaceRead-only	2249
このポリシーを使用すると	2249
ポリシーの詳細	2249
ポリシーのバージョン	2250
JSON ポリシードキュメント	2250
詳細はこちら	2251

AWSMarketplaceResaleAuthorizationServiceRolePolicy	2251
このポリシーを使用すると	2251
ポリシーの詳細	2252
ポリシーのバージョン	2252
JSON ポリシードキュメント	2252
詳細はこちら	2254
AWSMarketplaceSellerFullAccess	2254
このポリシーを使用すると	2255
ポリシーの詳細	2255
ポリシーのバージョン	2255
JSON ポリシードキュメント	2255
詳細はこちら	2258
AWSMarketplaceSellerProductsFullAccess	2259
このポリシーを使用すると	2259
ポリシーの詳細	2259
ポリシーのバージョン	2259
JSON ポリシードキュメント	2259
詳細はこちら	2261
AWSMarketplaceSellerProductsReadOnly	2261
このポリシーを使用すると	2262
ポリシーの詳細	2262
ポリシーのバージョン	2262
JSON ポリシードキュメント	2262
詳細はこちら	2263
AWSMediaConnectServicePolicy	2263
このポリシーを使用すると	2263
ポリシーの詳細	2263
ポリシーのバージョン	2264
JSON ポリシードキュメント	2264
詳細はこちら	2265
AWSMediaTailorServiceRolePolicy	2265
このポリシーを使用すると	2265
ポリシーの詳細	2265
ポリシーのバージョン	2266
JSON ポリシードキュメント	2266
詳細はこちら	2266

AWSMigrationHubDiscoveryAccess	2267
このポリシーを使用すると	2267
ポリシーの詳細	2267
ポリシーのバージョン	2267
JSON ポリシードキュメント	2267
詳細はこちら	2268
AWSMigrationHubDMSAccess	2269
このポリシーを使用すると	2269
ポリシーの詳細	2269
ポリシーのバージョン	2269
JSON ポリシードキュメント	2269
詳細はこちら	2270
AWSMigrationHubFullAccess	2270
このポリシーを使用すると	2271
ポリシーの詳細	2271
ポリシーのバージョン	2271
JSON ポリシードキュメント	2271
詳細はこちら	2272
AWSMigrationHubOrchestratorConsoleFullAccess	2273
このポリシーを使用すると	2273
ポリシーの詳細	2273
ポリシーのバージョン	2273
JSON ポリシードキュメント	2273
詳細はこちら	2276
AWSMigrationHubOrchestratorInstanceRolePolicy	2277
このポリシーを使用すると	2277
ポリシーの詳細	2277
ポリシーのバージョン	2277
JSON ポリシードキュメント	2277
詳細はこちら	2278
AWSMigrationHubOrchestratorPlugin	2278
このポリシーを使用すると	2278
ポリシーの詳細	2278
ポリシーのバージョン	2279
JSON ポリシードキュメント	2279
詳細はこちら	2280

AWSMigrationHubOrchestratorServiceRolePolicy	2280
このポリシーを使用すると	2281
ポリシーの詳細	2281
ポリシーのバージョン	2281
JSON ポリシードキュメント	2281
詳細はこちら	2285
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess	2285
このポリシーを使用すると	2285
ポリシーの詳細	2285
ポリシーのバージョン	2285
JSON ポリシードキュメント	2286
詳細はこちら	2291
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy	2291
このポリシーを使用すると	2292
ポリシーの詳細	2292
ポリシーのバージョン	2292
JSON ポリシードキュメント	2292
詳細はこちら	2294
AWSMigrationHubRefactorSpacesFullAccess	2294
このポリシーを使用すると	2294
ポリシーの詳細	2294
ポリシーのバージョン	2294
JSON ポリシードキュメント	2295
詳細はこちら	2301
AWSMigrationHubRefactorSpacesServiceRolePolicy	2301
このポリシーを使用すると	2301
ポリシーの詳細	2302
ポリシーのバージョン	2302
JSON ポリシードキュメント	2302
詳細はこちら	2306
AWSMigrationHubSMSAccess	2306
このポリシーを使用すると	2306
ポリシーの詳細	2306
ポリシーのバージョン	2306
JSON ポリシードキュメント	2306
詳細はこちら	2307

AWSMigrationHubStrategyCollector	2308
このポリシーを使用すると	2308
ポリシーの詳細	2308
ポリシーのバージョン	2308
JSON ポリシードキュメント	2308
詳細はこちら	2311
AWSMigrationHubStrategyConsoleFullAccess	2311
このポリシーを使用すると	2311
ポリシーの詳細	2311
ポリシーのバージョン	2311
JSON ポリシードキュメント	2312
詳細はこちら	2313
AWSMigrationHubStrategyServiceRolePolicy	2313
このポリシーを使用すると	2314
ポリシーの詳細	2314
ポリシーのバージョン	2314
JSON ポリシードキュメント	2314
詳細はこちら	2315
AWSMobileHub_FullAccess	2315
このポリシーを使用すると	2315
ポリシーの詳細	2316
ポリシーのバージョン	2316
JSON ポリシードキュメント	2316
詳細はこちら	2317
AWSMobileHub_ReadOnly	2318
このポリシーを使用すると	2318
ポリシーの詳細	2318
ポリシーのバージョン	2318
JSON ポリシードキュメント	2318
詳細はこちら	2319
AWSMSKReplicatorExecutionRole	2320
このポリシーを使用すると	2320
ポリシーの詳細	2320
ポリシーのバージョン	2320
JSON ポリシードキュメント	2320
詳細はこちら	2322

AWSNetworkFirewallServiceRolePolicy	2322
このポリシーを使用すると	2322
ポリシーの詳細	2322
ポリシーのバージョン	2322
JSON ポリシードキュメント	2323
詳細はこちら	2324
AWSNetworkManagerCloudWANServiceRolePolicy	2324
このポリシーを使用すると	2325
ポリシーの詳細	2325
ポリシーのバージョン	2325
JSON ポリシードキュメント	2325
詳細はこちら	2326
AWSNetworkManagerFullAccess	2326
このポリシーを使用すると	2326
ポリシーの詳細	2326
ポリシーのバージョン	2326
JSON ポリシードキュメント	2326
詳細はこちら	2327
AWSNetworkManagerReadOnlyAccess	2327
このポリシーを使用すると	2327
ポリシーの詳細	2328
ポリシーのバージョン	2328
JSON ポリシードキュメント	2328
詳細はこちら	2328
AWSNetworkManagerServiceRolePolicy	2329
このポリシーを使用すると	2329
ポリシーの詳細	2329
ポリシーのバージョン	2329
JSON ポリシードキュメント	2329
詳細はこちら	2330
AWSOpsWorks_FullAccess	2330
このポリシーを使用すると	2331
ポリシーの詳細	2331
ポリシーのバージョン	2331
JSON ポリシードキュメント	2331
詳細はこちら	2332

AWSOpsWorksCloudWatchLogs	2332
このポリシーを使用すると	2332
ポリシーの詳細	2333
ポリシーのバージョン	2333
JSON ポリシードキュメント	2333
詳細はこちら	2333
AWSOpsWorksCMInstanceProfileRole	2334
このポリシーを使用すると	2334
ポリシーの詳細	2334
ポリシーのバージョン	2334
JSON ポリシードキュメント	2334
詳細はこちら	2335
AWSOpsWorksCMServiceRole	2335
このポリシーを使用すると	2336
ポリシーの詳細	2336
ポリシーのバージョン	2336
JSON ポリシードキュメント	2336
詳細はこちら	2340
AWSOpsWorksInstanceRegistration	2340
このポリシーを使用すると	2341
ポリシーの詳細	2341
ポリシーのバージョン	2341
JSON ポリシードキュメント	2341
詳細はこちら	2342
AWSOpsWorksRegisterCLI_EC2	2342
このポリシーを使用すると	2342
ポリシーの詳細	2342
ポリシーのバージョン	2342
JSON ポリシードキュメント	2342
詳細はこちら	2343
AWSOpsWorksRegisterCLI_OnPremises	2343
このポリシーを使用すると	2344
ポリシーの詳細	2344
ポリシーのバージョン	2344
JSON ポリシードキュメント	2344
詳細はこちら	2346

AWSOrganizationsFullAccess	2346
このポリシーを使用すると	2346
ポリシーの詳細	2346
ポリシーのバージョン	2346
JSON ポリシードキュメント	2346
詳細はこちら	2347
AWSOrganizationsReadOnlyAccess	2348
このポリシーを使用すると	2348
ポリシーの詳細	2348
ポリシーのバージョン	2348
JSON ポリシードキュメント	2348
詳細はこちら	2349
AWSOrganizationsServiceTrustPolicy	2349
このポリシーを使用すると	2349
ポリシーの詳細	2349
ポリシーのバージョン	2350
JSON ポリシードキュメント	2350
詳細はこちら	2351
AWSOutpostsAuthorizeServerPolicy	2351
このポリシーを使用すると	2351
ポリシーの詳細	2351
ポリシーのバージョン	2351
JSON ポリシードキュメント	2351
詳細はこちら	2352
AWSOutpostsServiceRolePolicy	2352
このポリシーを使用すると	2352
ポリシーの詳細	2352
ポリシーのバージョン	2353
JSON ポリシードキュメント	2353
詳細はこちら	2353
AWSPanoramaApplianceRolePolicy	2353
このポリシーを使用すると	2354
ポリシーの詳細	2354
ポリシーのバージョン	2354
JSON ポリシードキュメント	2354
詳細はこちら	2355

AWSPanoramaApplianceServiceRolePolicy	2355
このポリシーを使用すると	2355
ポリシーの詳細	2355
ポリシーのバージョン	2355
JSON ポリシードキュメント	2356
詳細はこちら	2357
AWSPanoramaFullAccess	2357
このポリシーを使用すると	2357
ポリシーの詳細	2358
ポリシーのバージョン	2358
JSON ポリシードキュメント	2358
詳細はこちら	2360
AWSPanoramaGreengrassGroupRolePolicy	2361
このポリシーを使用すると	2361
ポリシーの詳細	2361
ポリシーのバージョン	2361
JSON ポリシードキュメント	2361
詳細はこちら	2363
AWSPanoramaSageMakerRolePolicy	2363
このポリシーを使用すると	2363
ポリシーの詳細	2363
ポリシーのバージョン	2363
JSON ポリシードキュメント	2364
詳細はこちら	2364
AWSPanoramaServiceLinkedRolePolicy	2364
このポリシーを使用すると	2364
ポリシーの詳細	2365
ポリシーのバージョン	2365
JSON ポリシードキュメント	2365
詳細はこちら	2368
AWSPanoramaServiceRolePolicy	2368
このポリシーを使用すると	2368
ポリシーの詳細	2368
ポリシーのバージョン	2368
JSON ポリシードキュメント	2368
詳細はこちら	2375

AWSPriceListServiceFullAccess	2376
このポリシーを使用すると	2376
ポリシーの詳細	2376
ポリシーのバージョン	2376
JSON ポリシードキュメント	2376
詳細はこちら	2377
AWSPrivateCAAuditor	2377
このポリシーを使用すると	2377
ポリシーの詳細	2377
ポリシーのバージョン	2377
JSON ポリシードキュメント	2377
詳細はこちら	2378
AWSPrivateCAFullAccess	2378
このポリシーを使用すると	2378
ポリシーの詳細	2379
ポリシーのバージョン	2379
JSON ポリシードキュメント	2379
詳細はこちら	2379
AWSPrivateCAPrivilegedUser	2380
このポリシーを使用すると	2380
ポリシーの詳細	2380
ポリシーのバージョン	2380
JSON ポリシードキュメント	2380
詳細はこちら	2381
AWSPrivateCAReadOnly	2382
このポリシーを使用すると	2382
ポリシーの詳細	2382
ポリシーのバージョン	2382
JSON ポリシードキュメント	2382
詳細はこちら	2383
AWSPrivateCAUser	2383
このポリシーを使用すると	2383
ポリシーの詳細	2383
ポリシーのバージョン	2383
JSON ポリシードキュメント	2384
詳細はこちら	2385

AWSPprivateMarketplaceAdminFullAccess	2385
このポリシーを使用すると	2385
ポリシーの詳細	2385
ポリシーのバージョン	2386
JSON ポリシードキュメント	2386
詳細はこちら	2387
AWSPprivateMarketplaceRequests	2387
このポリシーを使用すると	2388
ポリシーの詳細	2388
ポリシーのバージョン	2388
JSON ポリシードキュメント	2388
詳細はこちら	2388
AWSPprivateNetworksServiceRolePolicy	2389
このポリシーを使用すると	2389
ポリシーの詳細	2389
ポリシーのバージョン	2389
JSON ポリシードキュメント	2389
詳細はこちら	2390
AWSProtonCodeBuildProvisioningBasicAccess	2390
このポリシーを使用すると	2390
ポリシーの詳細	2390
ポリシーのバージョン	2391
JSON ポリシードキュメント	2391
詳細はこちら	2391
AWSProtonCodeBuildProvisioningServiceRolePolicy	2392
このポリシーを使用すると	2392
ポリシーの詳細	2392
ポリシーのバージョン	2392
JSON ポリシードキュメント	2392
詳細はこちら	2394
AWSProtonDeveloperAccess	2394
このポリシーを使用すると	2394
ポリシーの詳細	2394
ポリシーのバージョン	2394
JSON ポリシードキュメント	2394
詳細はこちら	2397

AWSProtonFullAccess	2397
このポリシーを使用すると	2397
ポリシーの詳細	2397
ポリシーのバージョン	2397
JSON ポリシードキュメント	2398
詳細はこちら	2400
AWSProtonReadOnlyAccess	2400
このポリシーを使用すると	2400
ポリシーの詳細	2400
ポリシーのバージョン	2400
JSON ポリシードキュメント	2401
詳細はこちら	2402
AWSProtonServiceGitSyncServiceRolePolicy	2402
このポリシーを使用すると	2402
ポリシーの詳細	2402
ポリシーのバージョン	2403
JSON ポリシードキュメント	2403
詳細はこちら	2404
AWSProtonSyncServiceRolePolicy	2404
このポリシーを使用すると	2404
ポリシーの詳細	2404
ポリシーのバージョン	2404
JSON ポリシードキュメント	2405
詳細はこちら	2406
AWSPurchaseOrdersServiceRolePolicy	2406
このポリシーを使用すると	2406
ポリシーの詳細	2406
ポリシーのバージョン	2406
JSON ポリシードキュメント	2406
詳細はこちら	2407
AWSQuickSightAssetBundleExportPolicy	2407
このポリシーを使用すると	2408
ポリシーの詳細	2408
ポリシーのバージョン	2408
JSON ポリシードキュメント	2408
詳細はこちら	2410

AWSQuickSightAssetBundleImportPolicy	2410
このポリシーを使用すると	2411
ポリシーの詳細	2411
ポリシーのバージョン	2411
JSON ポリシードキュメント	2411
詳細はこちら	2414
AWSQuickSightAthenaAccess	2414
このポリシーを使用すると	2414
ポリシーの詳細	2414
ポリシーのバージョン	2415
JSON ポリシードキュメント	2415
詳細はこちら	2417
AWSQuickSightDescribeRDS	2417
このポリシーを使用すると	2417
ポリシーの詳細	2417
ポリシーのバージョン	2418
JSON ポリシードキュメント	2418
詳細はこちら	2418
AWSQuickSightDescribeRedshift	2418
このポリシーを使用すると	2419
ポリシーの詳細	2419
ポリシーのバージョン	2419
JSON ポリシードキュメント	2419
詳細はこちら	2419
AWSQuickSightElasticsearchPolicy	2420
このポリシーを使用すると	2420
ポリシーの詳細	2420
ポリシーのバージョン	2420
JSON ポリシードキュメント	2420
詳細はこちら	2421
AWSQuickSightIoTAnalyticsAccess	2422
このポリシーを使用すると	2422
ポリシーの詳細	2422
ポリシーのバージョン	2422
JSON ポリシードキュメント	2422
詳細はこちら	2423

AWSQuickSightListIAM	2423
このポリシーを使用すると	2423
ポリシーの詳細	2423
ポリシーのバージョン	2423
JSON ポリシードキュメント	2424
詳細はこちら	2424
AWSQuickSightOpenSearchPolicy	2424
このポリシーを使用すると	2424
ポリシーの詳細	2424
ポリシーのバージョン	2425
JSON ポリシードキュメント	2425
詳細はこちら	2426
AWSQuickSightSageMakerPolicy	2426
このポリシーを使用すると	2426
ポリシーの詳細	2426
ポリシーのバージョン	2427
JSON ポリシードキュメント	2427
詳細はこちら	2428
AWSQuickSightTimestreamPolicy	2428
このポリシーを使用すると	2428
ポリシーの詳細	2428
ポリシーのバージョン	2429
JSON ポリシードキュメント	2429
詳細はこちら	2429
AWSReachabilityAnalyzerServiceRolePolicy	2430
このポリシーを使用すると	2430
ポリシーの詳細	2430
ポリシーのバージョン	2430
JSON ポリシードキュメント	2430
詳細はこちら	2433
AWSRefactoringToolkitFullAccess	2433
このポリシーを使用すると	2433
ポリシーの詳細	2433
ポリシーのバージョン	2433
JSON ポリシードキュメント	2434
詳細はこちら	2447

AWSRefactoringToolkitSidecarPolicy	2447
このポリシーを使用すると	2448
ポリシーの詳細	2448
ポリシーのバージョン	2448
JSON ポリシードキュメント	2448
詳細はこちら	2449
AWSrePostPrivateCloudWatchAccess	2449
このポリシーを使用すると	2449
ポリシーの詳細	2450
ポリシーのバージョン	2450
JSON ポリシードキュメント	2450
詳細はこちら	2451
AWSRepostSpaceSupportOperationsPolicy	2451
このポリシーを使用すると	2451
ポリシーの詳細	2451
ポリシーのバージョン	2451
JSON ポリシードキュメント	2451
詳細はこちら	2452
AWSResilienceHubAssessmentExecutionPolicy	2452
このポリシーを使用すると	2452
ポリシーの詳細	2452
ポリシーのバージョン	2453
JSON ポリシードキュメント	2453
詳細はこちら	2457
AWSResourceAccessManagerFullAccess	2457
このポリシーを使用すると	2457
ポリシーの詳細	2457
ポリシーのバージョン	2458
JSON ポリシードキュメント	2458
詳細はこちら	2458
AWSResourceAccessManagerReadOnlyAccess	2458
このポリシーを使用すると	2459
ポリシーの詳細	2459
ポリシーのバージョン	2459
JSON ポリシードキュメント	2459
詳細はこちら	2459

AWSResourceAccessManagerResourceShareParticipantAccess	2460
このポリシーを使用すると	2460
ポリシーの詳細	2460
ポリシーのバージョン	2460
JSON ポリシードキュメント	2460
詳細はこちら	2461
AWSResourceAccessManagerServiceRolePolicy	2461
このポリシーを使用すると	2461
ポリシーの詳細	2461
ポリシーのバージョン	2462
JSON ポリシードキュメント	2462
詳細はこちら	2463
AWSResourceExplorerFullAccess	2463
このポリシーを使用すると	2463
ポリシーの詳細	2463
ポリシーのバージョン	2463
JSON ポリシードキュメント	2464
詳細はこちら	2464
AWSResourceExplorerOrganizationsAccess	2465
このポリシーを使用すると	2465
ポリシーの詳細	2465
ポリシーのバージョン	2465
JSON ポリシードキュメント	2465
詳細はこちら	2467
AWSResourceExplorerReadOnlyAccess	2467
このポリシーを使用すると	2467
ポリシーの詳細	2467
ポリシーのバージョン	2468
JSON ポリシードキュメント	2468
詳細はこちら	2468
AWSResourceExplorerServiceRolePolicy	2469
このポリシーを使用すると	2469
ポリシーの詳細	2469
ポリシーのバージョン	2469
JSON ポリシードキュメント	2469
詳細はこちら	2478

AWSResourceGroupsReadOnlyAccess	2479
このポリシーを使用すると	2479
ポリシーの詳細	2479
ポリシーのバージョン	2479
JSON ポリシードキュメント	2479
詳細はこちら	2481
AWSRoboMaker_FullAccess	2481
このポリシーを使用すると	2481
ポリシーの詳細	2481
ポリシーのバージョン	2481
JSON ポリシードキュメント	2481
詳細はこちら	2483
AWSRoboMakerReadOnlyAccess	2483
このポリシーを使用すると	2483
ポリシーの詳細	2483
ポリシーのバージョン	2483
JSON ポリシードキュメント	2484
詳細はこちら	2484
AWSRoboMakerServicePolicy	2484
このポリシーを使用すると	2484
ポリシーの詳細	2485
ポリシーのバージョン	2485
JSON ポリシードキュメント	2485
詳細はこちら	2487
AWSRoboMakerServiceRolePolicy	2487
このポリシーを使用すると	2487
ポリシーの詳細	2487
ポリシーのバージョン	2487
JSON ポリシードキュメント	2487
詳細はこちら	2489
AWSRolesAnywhereServicePolicy	2489
このポリシーを使用すると	2489
ポリシーの詳細	2489
ポリシーのバージョン	2489
JSON ポリシードキュメント	2490
詳細はこちら	2490

AWSS3OnOutpostsServiceRolePolicy	2490
このポリシーを使用すると	2491
ポリシーの詳細	2491
ポリシーのバージョン	2491
JSON ポリシードキュメント	2491
詳細はこちら	2494
AWSSavingsPlansFullAccess	2494
このポリシーを使用すると	2494
ポリシーの詳細	2494
ポリシーのバージョン	2494
JSON ポリシードキュメント	2495
詳細はこちら	2495
AWSSavingsPlansReadOnlyAccess	2495
このポリシーを使用すると	2495
ポリシーの詳細	2495
ポリシーのバージョン	2496
JSON ポリシードキュメント	2496
詳細はこちら	2496
AWSSecurityHubFullAccess	2496
このポリシーを使用すると	2496
ポリシーの詳細	2497
ポリシーのバージョン	2497
JSON ポリシードキュメント	2497
詳細はこちら	2498
AWSSecurityHubOrganizationsAccess	2498
このポリシーを使用すると	2498
ポリシーの詳細	2498
ポリシーのバージョン	2499
JSON ポリシードキュメント	2499
詳細はこちら	2500
AWSSecurityHubReadOnlyAccess	2500
このポリシーを使用すると	2500
ポリシーの詳細	2500
ポリシーのバージョン	2501
JSON ポリシードキュメント	2501
詳細はこちら	2501

AWSSecurityHubServiceRolePolicy	2501
このポリシーを使用すると	2502
ポリシーの詳細	2502
ポリシーのバージョン	2502
JSON ポリシードキュメント	2502
詳細はこちら	2504
AWSServiceCatalogAdminFullAccess	2504
このポリシーを使用すると	2504
ポリシーの詳細	2505
ポリシーのバージョン	2505
JSON ポリシードキュメント	2505
詳細はこちら	2508
AWSServiceCatalogAdminReadOnlyAccess	2508
このポリシーを使用すると	2508
ポリシーの詳細	2508
ポリシーのバージョン	2508
JSON ポリシードキュメント	2509
詳細はこちら	2510
AWSServiceCatalogAppRegistryFullAccess	2510
このポリシーを使用すると	2510
ポリシーの詳細	2510
ポリシーのバージョン	2511
JSON ポリシードキュメント	2511
詳細はこちら	2513
AWSServiceCatalogAppRegistryReadOnlyAccess	2513
このポリシーを使用すると	2513
ポリシーの詳細	2513
ポリシーのバージョン	2514
JSON ポリシードキュメント	2514
詳細はこちら	2514
AWSServiceCatalogAppRegistryServiceRolePolicy	2515
このポリシーを使用すると	2515
ポリシーの詳細	2515
ポリシーのバージョン	2515
JSON ポリシードキュメント	2515
詳細はこちら	2517

AWSServiceCatalogEndUserFullAccess	2517
このポリシーを使用すると	2517
ポリシーの詳細	2517
ポリシーのバージョン	2517
JSON ポリシードキュメント	2517
詳細はこちら	2519
AWSServiceCatalogEndUserReadOnlyAccess	2520
このポリシーを使用すると	2520
ポリシーの詳細	2520
ポリシーのバージョン	2520
JSON ポリシードキュメント	2520
詳細はこちら	2522
AWSServiceCatalogOrgsDataSyncServiceRolePolicy	2522
このポリシーを使用すると	2522
ポリシーの詳細	2522
ポリシーのバージョン	2523
JSON ポリシードキュメント	2523
詳細はこちら	2523
AWSServiceCatalogSyncServiceRolePolicy	2524
このポリシーを使用すると	2524
ポリシーの詳細	2524
ポリシーのバージョン	2524
JSON ポリシードキュメント	2524
詳細はこちら	2525
AWSServiceRoleForAmazonEKSNodegroup	2526
このポリシーを使用すると	2526
ポリシーの詳細	2526
ポリシーのバージョン	2526
JSON ポリシードキュメント	2526
詳細はこちら	2530
AWSServiceRoleForAmazonQDeveloper	2531
このポリシーを使用すると	2531
ポリシーの詳細	2531
ポリシーのバージョン	2531
JSON ポリシードキュメント	2531
詳細はこちら	2532

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy	2532
このポリシーを使用すると	2532
ポリシーの詳細	2532
ポリシーのバージョン	2533
JSON ポリシードキュメント	2533
詳細はこちら	2533
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy	2533
このポリシーを使用すると	2534
ポリシーの詳細	2534
ポリシーのバージョン	2534
JSON ポリシードキュメント	2534
詳細はこちら	2535
AWSServiceRoleForCodeGuru-Profiler	2535
このポリシーを使用すると	2535
ポリシーの詳細	2535
ポリシーのバージョン	2535
JSON ポリシードキュメント	2536
詳細はこちら	2536
AWSServiceRoleForCodeWhispererPolicy	2536
このポリシーを使用すると	2536
ポリシーの詳細	2536
ポリシーのバージョン	2537
JSON ポリシードキュメント	2537
詳細はこちら	2539
AWSServiceRoleForEC2ScheduledInstances	2539
このポリシーを使用すると	2539
ポリシーの詳細	2539
ポリシーのバージョン	2539
JSON ポリシードキュメント	2540
詳細はこちら	2540
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy	2541
このポリシーを使用すると	2541
ポリシーの詳細	2541
ポリシーのバージョン	2541
JSON ポリシードキュメント	2541
詳細はこちら	2542

AWSServiceRoleForImageBuilder	2542
このポリシーを使用すると	2542
ポリシーの詳細	2542
ポリシーのバージョン	2542
JSON ポリシードキュメント	2543
詳細はこちら	2552
AWSServiceRoleForIoTSiteWise	2552
このポリシーを使用すると	2553
ポリシーの詳細	2553
ポリシーのバージョン	2553
JSON ポリシードキュメント	2553
詳細はこちら	2554
AWSServiceRoleForLogDeliveryPolicy	2555
このポリシーを使用すると	2555
ポリシーの詳細	2555
ポリシーのバージョン	2555
JSON ポリシードキュメント	2555
詳細はこちら	2556
AWSServiceRoleForMonitronPolicy	2556
このポリシーを使用すると	2556
ポリシーの詳細	2556
ポリシーのバージョン	2557
JSON ポリシードキュメント	2557
詳細はこちら	2557
AWSServiceRoleForNeptuneGraphPolicy	2557
このポリシーを使用すると	2558
ポリシーの詳細	2558
ポリシーのバージョン	2558
JSON ポリシードキュメント	2558
詳細はこちら	2559
AWSServiceRoleForPrivateMarketplaceAdminPolicy	2560
このポリシーを使用すると	2560
ポリシーの詳細	2560
ポリシーのバージョン	2560
JSON ポリシードキュメント	2560
詳細はこちら	2562

AWSServiceRoleForSMS	2562
このポリシーを使用すると	2562
ポリシーの詳細	2562
ポリシーのバージョン	2563
JSON ポリシードキュメント	2563
詳細はこちら	2569
AWSServiceRoleForUserSubscriptions	2570
このポリシーを使用すると	2570
ポリシーの詳細	2570
ポリシーのバージョン	2570
JSON ポリシードキュメント	2570
詳細はこちら	2571
AWSServiceRolePolicyForBackupReports	2571
このポリシーを使用すると	2571
ポリシーの詳細	2571
ポリシーのバージョン	2572
JSON ポリシードキュメント	2572
詳細はこちら	2573
AWSServiceRolePolicyForBackupRestoreTesting	2573
このポリシーを使用すると	2573
ポリシーの詳細	2574
ポリシーのバージョン	2574
JSON ポリシードキュメント	2574
詳細はこちら	2577
AWSShieldDRTAcessPolicy	2577
このポリシーを使用すると	2577
ポリシーの詳細	2577
ポリシーのバージョン	2577
JSON ポリシードキュメント	2578
詳細はこちら	2579
AWSShieldServiceRolePolicy	2579
このポリシーを使用すると	2579
ポリシーの詳細	2579
ポリシーのバージョン	2579
JSON ポリシードキュメント	2580
詳細はこちら	2580

AWSSSMForSAPServiceLinkedRolePolicy	2580
このポリシーを使用すると	2580
ポリシーの詳細	2581
ポリシーのバージョン	2581
JSON ポリシードキュメント	2581
詳細はこちら	2587
AWSSSMOpsInsightsServiceRolePolicy	2588
このポリシーを使用すると	2588
ポリシーの詳細	2588
ポリシーのバージョン	2588
JSON ポリシードキュメント	2588
詳細はこちら	2589
AWSSSODirectoryAdministrator	2589
このポリシーを使用すると	2589
ポリシーの詳細	2589
ポリシーのバージョン	2590
JSON ポリシードキュメント	2590
詳細はこちら	2590
AWSSSODirectoryReadOnly	2590
このポリシーを使用すると	2591
ポリシーの詳細	2591
ポリシーのバージョン	2591
JSON ポリシードキュメント	2591
詳細はこちら	2592
AWSSSOMasterAccountAdministrator	2592
このポリシーを使用すると	2592
ポリシーの詳細	2592
ポリシーのバージョン	2592
JSON ポリシードキュメント	2593
詳細はこちら	2594
AWSSSOMemberAccountAdministrator	2595
このポリシーを使用すると	2595
ポリシーの詳細	2595
ポリシーのバージョン	2595
JSON ポリシードキュメント	2595
詳細はこちら	2596

AWSSSOReadOnly	2597
このポリシーを使用すると	2597
ポリシーの詳細	2597
ポリシーのバージョン	2597
JSON ポリシードキュメント	2597
詳細はこちら	2598
AWSSSOServiceRolePolicy	2598
このポリシーを使用すると	2599
ポリシーの詳細	2599
ポリシーのバージョン	2599
JSON ポリシードキュメント	2599
詳細はこちら	2603
AWSSStepFunctionsConsoleFullAccess	2603
このポリシーを使用すると	2603
ポリシーの詳細	2603
ポリシーのバージョン	2603
JSON ポリシードキュメント	2603
詳細はこちら	2604
AWSSStepFunctionsFullAccess	2604
このポリシーを使用すると	2605
ポリシーの詳細	2605
ポリシーのバージョン	2605
JSON ポリシードキュメント	2605
詳細はこちら	2605
AWSSStepFunctionsReadOnlyAccess	2606
このポリシーを使用すると	2606
ポリシーの詳細	2606
ポリシーのバージョン	2606
JSON ポリシードキュメント	2606
詳細はこちら	2607
AWSSStorageGatewayFullAccess	2607
このポリシーを使用すると	2607
ポリシーの詳細	2607
ポリシーのバージョン	2608
JSON ポリシードキュメント	2608
詳細はこちら	2608

AWSSStorageGatewayReadOnlyAccess	2609
このポリシーを使用すると	2609
ポリシーの詳細	2609
ポリシーのバージョン	2609
JSON ポリシードキュメント	2609
詳細はこちら	2610
AWSSStorageGatewayServiceRolePolicy	2610
このポリシーを使用すると	2610
ポリシーの詳細	2611
ポリシーのバージョン	2611
JSON ポリシードキュメント	2611
詳細はこちら	2611
AWSSupplyChainFederationAdminAccess	2612
このポリシーを使用すると	2612
ポリシーの詳細	2612
ポリシーのバージョン	2612
JSON ポリシードキュメント	2612
詳細はこちら	2618
AWSSupportAccess	2618
このポリシーを使用すると	2618
ポリシーの詳細	2618
ポリシーのバージョン	2618
JSON ポリシードキュメント	2619
詳細はこちら	2619
AWSSupportAppFullAccess	2619
このポリシーを使用すると	2619
ポリシーの詳細	2619
ポリシーのバージョン	2620
JSON ポリシードキュメント	2620
詳細はこちら	2621
AWSSupportAppReadOnlyAccess	2621
このポリシーを使用すると	2621
ポリシーの詳細	2621
ポリシーのバージョン	2621
JSON ポリシードキュメント	2622
詳細はこちら	2622

AWSSupportPlansFullAccess	2622
このポリシーを使用すると	2622
ポリシーの詳細	2622
ポリシーのバージョン	2623
JSON ポリシードキュメント	2623
詳細はこちら	2623
AWSSupportPlansReadOnlyAccess	2623
このポリシーを使用すると	2624
ポリシーの詳細	2624
ポリシーのバージョン	2624
JSON ポリシードキュメント	2624
詳細はこちら	2624
AWSSupportServiceRolePolicy	2625
このポリシーを使用すると	2625
ポリシーの詳細	2625
ポリシーのバージョン	2625
JSON ポリシードキュメント	2625
詳細はこちら	2701
AWSSystemsManagerAccountDiscoveryServicePolicy	2701
このポリシーを使用すると	2701
ポリシーの詳細	2701
ポリシーのバージョン	2701
JSON ポリシードキュメント	2702
詳細はこちら	2702
AWSSystemsManagerChangeManagementServicePolicy	2702
このポリシーを使用すると	2703
ポリシーの詳細	2703
ポリシーのバージョン	2703
JSON ポリシードキュメント	2703
詳細はこちら	2705
AWSSystemsManagerForSAPFullAccess	2705
このポリシーを使用すると	2705
ポリシーの詳細	2705
ポリシーのバージョン	2705
JSON ポリシードキュメント	2706
詳細はこちら	2706

AWSSystemsManagerForSAPReadOnlyAccess	2707
このポリシーを使用すると	2707
ポリシーの詳細	2707
ポリシーのバージョン	2707
JSON ポリシードキュメント	2707
詳細はこちら	2708
AWSSystemsManagerOpsDataSyncServiceRolePolicy	2708
このポリシーを使用すると	2708
ポリシーの詳細	2708
ポリシーのバージョン	2708
JSON ポリシードキュメント	2709
詳細はこちら	2712
AWSThinkboxAssetServerPolicy	2712
このポリシーを使用すると	2712
ポリシーの詳細	2713
ポリシーのバージョン	2713
JSON ポリシードキュメント	2713
詳細はこちら	2714
AWSThinkboxAWSPortalAdminPolicy	2714
このポリシーを使用すると	2714
ポリシーの詳細	2714
ポリシーのバージョン	2714
JSON ポリシードキュメント	2715
詳細はこちら	2724
AWSThinkboxAWSPortalGatewayPolicy	2725
このポリシーを使用すると	2725
ポリシーの詳細	2725
ポリシーのバージョン	2725
JSON ポリシードキュメント	2725
詳細はこちら	2727
AWSThinkboxAWSPortalWorkerPolicy	2727
このポリシーを使用すると	2727
ポリシーの詳細	2728
ポリシーのバージョン	2728
JSON ポリシードキュメント	2728
詳細はこちら	2730

AWSThinkboxDeadlineResourceTrackerAccessPolicy	2730
このポリシーを使用すると	2730
ポリシーの詳細	2730
ポリシーのバージョン	2731
JSON ポリシードキュメント	2731
詳細はこちら	2734
AWSThinkboxDeadlineResourceTrackerAdminPolicy	2734
このポリシーを使用すると	2734
ポリシーの詳細	2734
ポリシーのバージョン	2734
JSON ポリシードキュメント	2735
詳細はこちら	2740
AWSThinkboxDeadlineSpotEventPluginAdminPolicy	2741
このポリシーを使用すると	2741
ポリシーの詳細	2741
ポリシーのバージョン	2741
JSON ポリシードキュメント	2741
詳細はこちら	2744
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy	2744
このポリシーを使用すると	2744
ポリシーの詳細	2745
ポリシーのバージョン	2745
JSON ポリシードキュメント	2745
詳細はこちら	2746
AWSTransferConsoleFullAccess	2747
このポリシーを使用すると	2747
ポリシーの詳細	2747
ポリシーのバージョン	2747
JSON ポリシードキュメント	2747
詳細はこちら	2748
AWSTransferFullAccess	2748
このポリシーを使用すると	2748
ポリシーの詳細	2749
ポリシーのバージョン	2749
JSON ポリシードキュメント	2749
詳細はこちら	2750

AWSTransferLoggingAccess	2750
このポリシーを使用すると	2750
ポリシーの詳細	2750
ポリシーのバージョン	2750
JSON ポリシードキュメント	2751
詳細はこちら	2751
AWSTransferReadOnlyAccess	2751
このポリシーを使用すると	2751
ポリシーの詳細	2752
ポリシーのバージョン	2752
JSON ポリシードキュメント	2752
詳細はこちら	2752
AWSTrustedAdvisorPriorityFullAccess	2753
このポリシーを使用すると	2753
ポリシーの詳細	2753
ポリシーのバージョン	2753
JSON ポリシードキュメント	2753
詳細はこちら	2755
AWSTrustedAdvisorPriorityReadOnlyAccess	2755
このポリシーを使用すると	2756
ポリシーの詳細	2756
ポリシーのバージョン	2756
JSON ポリシードキュメント	2756
詳細はこちら	2757
AWSTrustedAdvisorReportingServiceRolePolicy	2757
このポリシーを使用すると	2757
ポリシーの詳細	2758
ポリシーのバージョン	2758
JSON ポリシードキュメント	2758
詳細はこちら	2759
AWSTrustedAdvisorServiceRolePolicy	2759
このポリシーを使用すると	2759
ポリシーの詳細	2759
ポリシーのバージョン	2759
JSON ポリシードキュメント	2759
詳細はこちら	2762

AWSUserNotificationsServiceLinkedRolePolicy	2762
このポリシーを使用すると	2763
ポリシーの詳細	2763
ポリシーのバージョン	2763
JSON ポリシードキュメント	2763
詳細はこちら	2764
AWSVendorInsightsAssessorFullAccess	2764
このポリシーを使用すると	2764
ポリシーの詳細	2764
ポリシーのバージョン	2765
JSON ポリシードキュメント	2765
詳細はこちら	2766
AWSVendorInsightsAssessorReadOnly	2766
このポリシーを使用すると	2766
ポリシーの詳細	2766
ポリシーのバージョン	2767
JSON ポリシードキュメント	2767
詳細はこちら	2767
AWSVendorInsightsVendorFullAccess	2768
このポリシーを使用すると	2768
ポリシーの詳細	2768
ポリシーのバージョン	2768
JSON ポリシードキュメント	2768
詳細はこちら	2770
AWSVendorInsightsVendorReadOnly	2770
このポリシーを使用すると	2770
ポリシーの詳細	2770
ポリシーのバージョン	2771
JSON ポリシードキュメント	2771
詳細はこちら	2772
AWSVpcLatticeServiceRolePolicy	2772
このポリシーを使用すると	2772
ポリシーの詳細	2772
ポリシーのバージョン	2772
JSON ポリシードキュメント	2773
詳細はこちら	2773

AWSVPCS2SVpnServiceRolePolicy	2773
このポリシーを使用すると	2773
ポリシーの詳細	2774
ポリシーのバージョン	2774
JSON ポリシードキュメント	2774
詳細はこちら	2774
AWSVPCTransitGatewayServiceRolePolicy	2775
このポリシーを使用すると	2775
ポリシーの詳細	2775
ポリシーのバージョン	2775
JSON ポリシードキュメント	2775
詳細はこちら	2776
AWSVPCVerifiedAccessServiceRolePolicy	2776
このポリシーを使用すると	2776
ポリシーの詳細	2776
ポリシーのバージョン	2777
JSON ポリシードキュメント	2777
詳細はこちら	2778
AWSWAFConsoleFullAccess	2778
このポリシーを使用すると	2779
ポリシーの詳細	2779
ポリシーのバージョン	2779
JSON ポリシードキュメント	2779
詳細はこちら	2781
AWSWAFConsoleReadOnlyAccess	2781
このポリシーを使用すると	2782
ポリシーの詳細	2782
ポリシーのバージョン	2782
JSON ポリシードキュメント	2782
詳細はこちら	2783
AWSWAFFullAccess	2783
このポリシーを使用すると	2783
ポリシーの詳細	2784
ポリシーのバージョン	2784
JSON ポリシードキュメント	2784
詳細はこちら	2786

AWSWAFReadOnlyAccess	2786
このポリシーを使用すると	2786
ポリシーの詳細	2786
ポリシーのバージョン	2786
JSON ポリシードキュメント	2786
詳細はこちら	2787
AWSWellArchitectedDiscoveryServiceRolePolicy	2787
このポリシーを使用すると	2788
ポリシーの詳細	2788
ポリシーのバージョン	2788
JSON ポリシードキュメント	2788
詳細はこちら	2790
AWSWellArchitectedOrganizationsServiceRolePolicy	2790
このポリシーを使用すると	2790
ポリシーの詳細	2790
ポリシーのバージョン	2790
JSON ポリシードキュメント	2790
詳細はこちら	2791
AWSWickrFullAccess	2791
このポリシーを使用すると	2791
ポリシーの詳細	2791
ポリシーのバージョン	2792
JSON ポリシードキュメント	2792
詳細はこちら	2792
AWSXrayCrossAccountSharingConfiguration	2792
このポリシーを使用すると	2793
ポリシーの詳細	2793
ポリシーのバージョン	2793
JSON ポリシードキュメント	2793
詳細はこちら	2794
AWSXRayDaemonWriteAccess	2794
このポリシーを使用すると	2794
ポリシーの詳細	2794
ポリシーのバージョン	2795
JSON ポリシードキュメント	2795
詳細はこちら	2795

AWSXrayFullAccess	2796
このポリシーを使用すると	2796
ポリシーの詳細	2796
ポリシーのバージョン	2796
JSON ポリシードキュメント	2796
詳細はこちら	2797
AWSXrayReadOnlyAccess	2797
このポリシーを使用すると	2797
ポリシーの詳細	2797
ポリシーのバージョン	2797
JSON ポリシードキュメント	2798
詳細はこちら	2798
AWSXrayWriteOnlyAccess	2799
このポリシーを使用すると	2799
ポリシーの詳細	2799
ポリシーのバージョン	2799
JSON ポリシードキュメント	2799
詳細はこちら	2800
AWSZonalAutoshiftPracticeRunSLRPolicy	2800
このポリシーを使用すると	2800
ポリシーの詳細	2800
ポリシーのバージョン	2800
JSON ポリシードキュメント	2801
詳細はこちら	2801
BatchServiceRolePolicy	2802
このポリシーを使用すると	2802
ポリシーの詳細	2802
ポリシーのバージョン	2802
JSON ポリシードキュメント	2802
詳細はこちら	2808
Billing	2808
このポリシーを使用すると	2809
ポリシーの詳細	2809
ポリシーのバージョン	2809
JSON ポリシードキュメント	2809
詳細はこちら	2812

CertificateManagerServiceRolePolicy	2812
このポリシーを使用すると	2812
ポリシーの詳細	2812
ポリシーのバージョン	2813
JSON ポリシードキュメント	2813
詳細はこちら	2813
ClientVPNServiceConnectionsRolePolicy	2813
このポリシーを使用すると	2814
ポリシーの詳細	2814
ポリシーのバージョン	2814
JSON ポリシードキュメント	2814
詳細はこちら	2815
ClientVPNServiceRolePolicy	2815
このポリシーを使用すると	2815
ポリシーの詳細	2815
ポリシーのバージョン	2815
JSON ポリシードキュメント	2815
詳細はこちら	2816
CloudFormationStackSetsOrgAdminServiceRolePolicy	2816
このポリシーを使用すると	2817
ポリシーの詳細	2817
ポリシーのバージョン	2817
JSON ポリシードキュメント	2817
詳細はこちら	2818
CloudFormationStackSetsOrgMemberServiceRolePolicy	2818
このポリシーを使用すると	2818
ポリシーの詳細	2818
ポリシーのバージョン	2818
JSON ポリシードキュメント	2819
詳細はこちら	2819
CloudFrontFullAccess	2820
このポリシーを使用すると	2820
ポリシーの詳細	2820
ポリシーのバージョン	2820
JSON ポリシードキュメント	2820
詳細はこちら	2821

CloudFrontReadOnlyAccess	2822
このポリシーを使用すると	2822
ポリシーの詳細	2822
ポリシーのバージョン	2822
JSON ポリシードキュメント	2822
詳細はこちら	2823
CloudHSMServiceRolePolicy	2823
このポリシーを使用すると	2823
ポリシーの詳細	2823
ポリシーのバージョン	2824
JSON ポリシードキュメント	2824
詳細はこちら	2824
CloudSearchFullAccess	2824
このポリシーを使用すると	2825
ポリシーの詳細	2825
ポリシーのバージョン	2825
JSON ポリシードキュメント	2825
詳細はこちら	2825
CloudSearchReadOnlyAccess	2826
このポリシーを使用すると	2826
ポリシーの詳細	2826
ポリシーのバージョン	2826
JSON ポリシードキュメント	2826
詳細はこちら	2827
CloudTrailServiceRolePolicy	2827
このポリシーを使用すると	2827
ポリシーの詳細	2827
ポリシーのバージョン	2827
JSON ポリシードキュメント	2828
詳細はこちら	2829
CloudWatch-CrossAccountAccess	2829
このポリシーを使用すると	2830
ポリシーの詳細	2830
ポリシーのバージョン	2830
JSON ポリシードキュメント	2830
詳細はこちら	2831

CloudWatchActionsEC2Access	2831
このポリシーを使用すると	2831
ポリシーの詳細	2831
ポリシーのバージョン	2831
JSON ポリシードキュメント	2831
詳細はこちら	2832
CloudWatchAgentAdminPolicy	2832
このポリシーを使用すると	2832
ポリシーの詳細	2832
ポリシーのバージョン	2833
JSON ポリシードキュメント	2833
詳細はこちら	2834
CloudWatchAgentServerPolicy	2834
このポリシーを使用すると	2834
ポリシーの詳細	2834
ポリシーのバージョン	2834
JSON ポリシードキュメント	2834
詳細はこちら	2835
CloudWatchApplicationInsightsFullAccess	2836
このポリシーを使用すると	2836
ポリシーの詳細	2836
ポリシーのバージョン	2836
JSON ポリシードキュメント	2836
詳細はこちら	2838
CloudWatchApplicationInsightsReadOnlyAccess	2838
このポリシーを使用すると	2838
ポリシーの詳細	2838
ポリシーのバージョン	2838
JSON ポリシードキュメント	2838
詳細はこちら	2839
CloudwatchApplicationInsightsServiceLinkedRolePolicy	2839
このポリシーを使用すると	2839
ポリシーの詳細	2839
ポリシーのバージョン	2840
JSON ポリシードキュメント	2840
詳細はこちら	2849

CloudWatchApplicationSignalsFullAccess	2850
このポリシーを使用すると	2850
ポリシーの詳細	2850
ポリシーのバージョン	2850
JSON ポリシードキュメント	2850
詳細はこちら	2853
CloudWatchApplicationSignalsReadOnlyAccess	2853
このポリシーを使用すると	2854
ポリシーの詳細	2854
ポリシーのバージョン	2854
JSON ポリシードキュメント	2854
詳細はこちら	2856
CloudWatchApplicationSignalsServiceRolePolicy	2857
このポリシーを使用すると	2857
ポリシーの詳細	2857
ポリシーのバージョン	2857
JSON ポリシードキュメント	2857
詳細はこちら	2860
CloudWatchAutomaticDashboardsAccess	2860
このポリシーを使用すると	2860
ポリシーの詳細	2860
ポリシーのバージョン	2860
JSON ポリシードキュメント	2860
詳細はこちら	2862
CloudWatchCrossAccountSharingConfiguration	2862
このポリシーを使用すると	2862
ポリシーの詳細	2862
ポリシーのバージョン	2862
JSON ポリシードキュメント	2863
詳細はこちら	2864
CloudWatchEventsBuiltInTargetExecutionAccess	2864
このポリシーを使用すると	2864
ポリシーの詳細	2864
ポリシーのバージョン	2864
JSON ポリシードキュメント	2865
詳細はこちら	2865

CloudWatchEventsFullAccess	2865
このポリシーを使用すると	2865
ポリシーの詳細	2865
ポリシーのバージョン	2866
JSON ポリシードキュメント	2866
詳細はこちら	2868
CloudWatchEventsInvocationAccess	2868
このポリシーを使用すると	2868
ポリシーの詳細	2868
ポリシーのバージョン	2869
JSON ポリシードキュメント	2869
詳細はこちら	2869
CloudWatchEventsReadOnlyAccess	2869
このポリシーを使用すると	2869
ポリシーの詳細	2870
ポリシーのバージョン	2870
JSON ポリシードキュメント	2870
詳細はこちら	2871
CloudWatchEventsServiceRolePolicy	2872
このポリシーを使用すると	2872
ポリシーの詳細	2872
ポリシーのバージョン	2872
JSON ポリシードキュメント	2872
詳細はこちら	2873
CloudWatchFullAccess	2873
このポリシーを使用すると	2873
ポリシーの詳細	2873
ポリシーのバージョン	2873
JSON ポリシードキュメント	2874
詳細はこちら	2875
CloudWatchFullAccessV2	2875
このポリシーを使用すると	2875
ポリシーの詳細	2875
ポリシーのバージョン	2875
JSON ポリシードキュメント	2875
詳細はこちら	2877

CloudWatchInternetMonitorServiceRolePolicy	2877
このポリシーを使用すると	2877
ポリシーの詳細	2878
ポリシーのバージョン	2878
JSON ポリシードキュメント	2878
詳細はこちら	2879
CloudWatchLambdaInsightsExecutionRolePolicy	2879
このポリシーを使用すると	2879
ポリシーの詳細	2879
ポリシーのバージョン	2880
JSON ポリシードキュメント	2880
詳細はこちら	2880
CloudWatchLogsCrossAccountSharingConfiguration	2881
このポリシーを使用すると	2881
ポリシーの詳細	2881
ポリシーのバージョン	2881
JSON ポリシードキュメント	2881
詳細はこちら	2882
CloudWatchLogsFullAccess	2882
このポリシーを使用すると	2882
ポリシーの詳細	2883
ポリシーのバージョン	2883
JSON ポリシードキュメント	2883
詳細はこちら	2883
CloudWatchLogsReadOnlyAccess	2884
このポリシーを使用すると	2884
ポリシーの詳細	2884
ポリシーのバージョン	2884
JSON ポリシードキュメント	2884
詳細はこちら	2885
CloudWatchNetworkMonitorServiceRolePolicy	2885
このポリシーを使用すると	2885
ポリシーの詳細	2885
ポリシーのバージョン	2886
JSON ポリシードキュメント	2886
詳細はこちら	2887

CloudWatchReadOnlyAccess	2887
このポリシーを使用すると	2887
ポリシーの詳細	2887
ポリシーのバージョン	2888
JSON ポリシードキュメント	2888
詳細はこちら	2889
CloudWatchSyntheticsFullAccess	2889
このポリシーを使用すると	2889
ポリシーの詳細	2890
ポリシーのバージョン	2890
JSON ポリシードキュメント	2890
詳細はこちら	2895
CloudWatchSyntheticsReadOnlyAccess	2895
このポリシーを使用すると	2895
ポリシーの詳細	2895
ポリシーのバージョン	2895
JSON ポリシードキュメント	2895
詳細はこちら	2896
ComprehendDataAccessRolePolicy	2896
このポリシーを使用すると	2896
ポリシーの詳細	2896
ポリシーのバージョン	2897
JSON ポリシードキュメント	2897
詳細はこちら	2897
ComprehendFullAccess	2897
このポリシーを使用すると	2898
ポリシーの詳細	2898
ポリシーのバージョン	2898
JSON ポリシードキュメント	2898
詳細はこちら	2899
ComprehendMedicalFullAccess	2899
このポリシーを使用すると	2899
ポリシーの詳細	2899
ポリシーのバージョン	2899
JSON ポリシードキュメント	2899
詳細はこちら	2900

ComprehendReadOnly	2900
このポリシーを使用すると	2900
ポリシーの詳細	2900
ポリシーのバージョン	2900
JSON ポリシードキュメント	2901
詳細はこちら	2902
ComputeOptimizerReadOnlyAccess	2902
このポリシーを使用すると	2902
ポリシーの詳細	2902
ポリシーのバージョン	2903
JSON ポリシードキュメント	2903
詳細はこちら	2904
ComputeOptimizerServiceRolePolicy	2904
このポリシーを使用すると	2904
ポリシーの詳細	2904
ポリシーのバージョン	2904
JSON ポリシードキュメント	2905
詳細はこちら	2906
ConfigConformsServiceRolePolicy	2906
このポリシーを使用すると	2906
ポリシーの詳細	2906
ポリシーのバージョン	2907
JSON ポリシードキュメント	2907
詳細はこちら	2910
CostOptimizationHubAdminAccess	2910
このポリシーを使用すると	2910
ポリシーの詳細	2910
ポリシーのバージョン	2910
JSON ポリシードキュメント	2910
詳細はこちら	2912
CostOptimizationHubReadOnlyAccess	2912
このポリシーを使用すると	2912
ポリシーの詳細	2912
ポリシーのバージョン	2912
JSON ポリシードキュメント	2913
詳細はこちら	2913

CostOptimizationHubServiceRolePolicy	2913
このポリシーを使用すると	2913
ポリシーの詳細	2914
ポリシーのバージョン	2914
JSON ポリシードキュメント	2914
詳細はこちら	2915
CustomerProfilesServiceLinkedRolePolicy	2915
このポリシーを使用すると	2915
ポリシーの詳細	2915
ポリシーのバージョン	2915
JSON ポリシードキュメント	2916
詳細はこちら	2916
DatabaseAdministrator	2917
このポリシーを使用すると	2917
ポリシーの詳細	2917
ポリシーのバージョン	2917
JSON ポリシードキュメント	2917
詳細はこちら	2920
DataScientist	2920
このポリシーを使用すると	2920
ポリシーの詳細	2920
ポリシーのバージョン	2920
JSON ポリシードキュメント	2920
詳細はこちら	2924
DAXServiceRolePolicy	2924
このポリシーを使用すると	2925
ポリシーの詳細	2925
ポリシーのバージョン	2925
JSON ポリシードキュメント	2925
詳細はこちら	2926
DynamoDBCloudWatchContributorInsightsServiceRolePolicy	2926
このポリシーを使用すると	2926
ポリシーの詳細	2926
ポリシーのバージョン	2926
JSON ポリシードキュメント	2927
詳細はこちら	2927

DynamoDBKinesisReplicationServiceRolePolicy	2927
このポリシーを使用すると	2928
ポリシーの詳細	2928
ポリシーのバージョン	2928
JSON ポリシードキュメント	2928
詳細はこちら	2929
DynamoDBReplicationServiceRolePolicy	2929
このポリシーを使用すると	2929
ポリシーの詳細	2929
ポリシーのバージョン	2929
JSON ポリシードキュメント	2930
詳細はこちら	2931
EC2FastLaunchFullAccess	2931
このポリシーを使用すると	2931
ポリシーの詳細	2931
ポリシーのバージョン	2931
JSON ポリシードキュメント	2932
詳細はこちら	2934
EC2FastLaunchServiceRolePolicy	2934
このポリシーを使用すると	2935
ポリシーの詳細	2935
ポリシーのバージョン	2935
JSON ポリシードキュメント	2935
詳細はこちら	2939
EC2FleetTimeShiftableServiceRolePolicy	2939
このポリシーを使用すると	2939
ポリシーの詳細	2939
ポリシーのバージョン	2940
JSON ポリシードキュメント	2940
詳細はこちら	2941
Ec2ImageBuilderCrossAccountDistributionAccess	2941
このポリシーを使用すると	2942
ポリシーの詳細	2942
ポリシーのバージョン	2942
JSON ポリシードキュメント	2942
詳細はこちら	2943

EC2ImageBuilderLifecycleExecutionPolicy	2943
このポリシーを使用すると	2943
ポリシーの詳細	2943
ポリシーのバージョン	2943
JSON ポリシードキュメント	2944
詳細はこちら	2946
EC2InstanceConnect	2946
このポリシーを使用すると	2946
ポリシーの詳細	2946
ポリシーのバージョン	2946
JSON ポリシードキュメント	2946
詳細はこちら	2947
Ec2InstanceConnectEndpoint	2947
このポリシーを使用すると	2947
ポリシーの詳細	2947
ポリシーのバージョン	2948
JSON ポリシードキュメント	2948
詳細はこちら	2950
EC2InstanceProfileForImageBuilder	2950
このポリシーを使用すると	2950
ポリシーの詳細	2950
ポリシーのバージョン	2950
JSON ポリシードキュメント	2951
詳細はこちら	2952
EC2InstanceProfileForImageBuilderECRContainerBuilds	2952
このポリシーを使用すると	2952
ポリシーの詳細	2952
ポリシーのバージョン	2953
JSON ポリシードキュメント	2953
詳細はこちら	2954
ECRReplicationServiceRolePolicy	2954
このポリシーを使用すると	2954
ポリシーの詳細	2955
ポリシーのバージョン	2955
JSON ポリシードキュメント	2955
詳細はこちら	2955

ElastiCacheServiceRolePolicy	2956
このポリシーを使用すると	2956
ポリシーの詳細	2956
ポリシーのバージョン	2956
JSON ポリシードキュメント	2956
詳細はこちら	2958
ElasticLoadBalancingFullAccess	2958
このポリシーを使用すると	2959
ポリシーの詳細	2959
ポリシーのバージョン	2959
JSON ポリシードキュメント	2959
詳細はこちら	2960
ElasticLoadBalancingReadOnly	2961
このポリシーを使用すると	2961
ポリシーの詳細	2961
ポリシーのバージョン	2961
JSON ポリシードキュメント	2961
詳細はこちら	2962
ElementalActivationsDownloadSoftwareAccess	2962
このポリシーを使用すると	2963
ポリシーの詳細	2963
ポリシーのバージョン	2963
JSON ポリシードキュメント	2963
詳細はこちら	2963
ElementalActivationsFullAccess	2964
このポリシーを使用すると	2964
ポリシーの詳細	2964
ポリシーのバージョン	2964
JSON ポリシードキュメント	2964
詳細はこちら	2965
ElementalActivationsGenerateLicenses	2965
このポリシーを使用すると	2965
ポリシーの詳細	2965
ポリシーのバージョン	2965
JSON ポリシードキュメント	2966
詳細はこちら	2966

ElementalActivationsReadOnlyAccess	2966
このポリシーを使用すると	2967
ポリシーの詳細	2967
ポリシーのバージョン	2967
JSON ポリシードキュメント	2967
詳細はこちら	2967
ElementalAppliancesSoftwareFullAccess	2968
このポリシーを使用すると	2968
ポリシーの詳細	2968
ポリシーのバージョン	2968
JSON ポリシードキュメント	2968
詳細はこちら	2969
ElementalAppliancesSoftwareReadOnlyAccess	2969
このポリシーを使用すると	2969
ポリシーの詳細	2969
ポリシーのバージョン	2969
JSON ポリシードキュメント	2970
詳細はこちら	2970
ElementalSupportCenterFullAccess	2970
このポリシーを使用すると	2970
ポリシーの詳細	2971
ポリシーのバージョン	2971
JSON ポリシードキュメント	2971
詳細はこちら	2971
EMRDescribeClusterPolicyForEMRWAL	2972
このポリシーを使用すると	2972
ポリシーの詳細	2972
ポリシーのバージョン	2972
JSON ポリシードキュメント	2972
詳細はこちら	2973
FMSServiceRolePolicy	2973
このポリシーを使用すると	2973
ポリシーの詳細	2973
ポリシーのバージョン	2973
JSON ポリシードキュメント	2974
詳細はこちら	2990

FSxDeleteServiceLinkedRoleAccess	2990
このポリシーを使用すると	2990
ポリシーの詳細	2990
ポリシーのバージョン	2990
JSON ポリシードキュメント	2991
詳細はこちら	2991
GameLiftGameServerGroupPolicy	2991
このポリシーを使用すると	2991
ポリシーの詳細	2991
ポリシーのバージョン	2992
JSON ポリシードキュメント	2992
詳細はこちら	2993
GlobalAcceleratorFullAccess	2994
このポリシーを使用すると	2994
ポリシーの詳細	2994
ポリシーのバージョン	2994
JSON ポリシードキュメント	2994
詳細はこちら	2995
GlobalAcceleratorReadOnlyAccess	2995
このポリシーを使用すると	2996
ポリシーの詳細	2996
ポリシーのバージョン	2996
JSON ポリシードキュメント	2996
詳細はこちら	2996
GreengrassOTAUpdateArtifactAccess	2997
このポリシーを使用すると	2997
ポリシーの詳細	2997
ポリシーのバージョン	2997
JSON ポリシードキュメント	2997
詳細はこちら	2998
GroundTruthSyntheticConsoleFullAccess	2998
このポリシーを使用すると	2998
ポリシーの詳細	2998
ポリシーのバージョン	2999
JSON ポリシードキュメント	2999
詳細はこちら	2999

GroundTruthSyntheticConsoleReadOnlyAccess	2999
このポリシーを使用すると	3000
ポリシーの詳細	3000
ポリシーのバージョン	3000
JSON ポリシードキュメント	3000
詳細はこちら	3001
Health_OrganizationsServiceRolePolicy	3001
このポリシーを使用すると	3001
ポリシーの詳細	3001
ポリシーのバージョン	3001
JSON ポリシードキュメント	3002
詳細はこちら	3002
IAMAccessAdvisorReadOnly	3002
このポリシーを使用すると	3002
ポリシーの詳細	3002
ポリシーのバージョン	3003
JSON ポリシードキュメント	3003
詳細はこちら	3004
IAMAccessAnalyzerFullAccess	3004
このポリシーを使用すると	3004
ポリシーの詳細	3004
ポリシーのバージョン	3004
JSON ポリシードキュメント	3005
詳細はこちら	3006
IAMAccessAnalyzerReadOnlyAccess	3006
このポリシーを使用すると	3006
ポリシーの詳細	3006
ポリシーのバージョン	3006
JSON ポリシードキュメント	3006
詳細はこちら	3007
IAMFullAccess	3007
このポリシーを使用すると	3007
ポリシーの詳細	3007
ポリシーのバージョン	3008
JSON ポリシードキュメント	3008
詳細はこちら	3008

IAMReadOnlyAccess	3009
このポリシーを使用すると	3009
ポリシーの詳細	3009
ポリシーのバージョン	3009
JSON ポリシードキュメント	3009
詳細はこちら	3010
IAMSelfManageServiceSpecificCredentials	3010
このポリシーを使用すると	3010
ポリシーの詳細	3010
ポリシーのバージョン	3010
JSON ポリシードキュメント	3011
詳細はこちら	3011
IAMUserChangePassword	3011
このポリシーを使用すると	3011
ポリシーの詳細	3012
ポリシーのバージョン	3012
JSON ポリシードキュメント	3012
詳細はこちら	3013
IAMUserSSHKeys	3013
このポリシーを使用すると	3013
ポリシーの詳細	3013
ポリシーのバージョン	3013
JSON ポリシードキュメント	3013
詳細はこちら	3014
IVSFullAccess	3014
このポリシーを使用すると	3014
ポリシーの詳細	3014
ポリシーのバージョン	3015
JSON ポリシードキュメント	3015
詳細はこちら	3015
IVSReadOnlyAccess	3015
このポリシーを使用すると	3016
ポリシーの詳細	3016
ポリシーのバージョン	3016
JSON ポリシードキュメント	3016
詳細はこちら	3017

IVSRecordToS3	3017
このポリシーを使用すると	3017
ポリシーの詳細	3018
ポリシーのバージョン	3018
JSON ポリシードキュメント	3018
詳細はこちら	3018
KafkaConnectServiceRolePolicy	3019
このポリシーを使用すると	3019
ポリシーの詳細	3019
ポリシーのバージョン	3019
JSON ポリシードキュメント	3019
詳細はこちら	3021
KafkaServiceRolePolicy	3021
このポリシーを使用すると	3021
ポリシーの詳細	3021
ポリシーのバージョン	3021
JSON ポリシードキュメント	3022
詳細はこちら	3023
KeyspacesReplicationServiceRolePolicy	3023
このポリシーを使用すると	3023
ポリシーの詳細	3023
ポリシーのバージョン	3024
JSON ポリシードキュメント	3024
詳細はこちら	3024
LakeFormationDataAccessServiceRolePolicy	3024
このポリシーを使用すると	3025
ポリシーの詳細	3025
ポリシーのバージョン	3025
JSON ポリシードキュメント	3025
詳細はこちら	3026
LexBotPolicy	3026
このポリシーを使用すると	3026
ポリシーの詳細	3026
ポリシーのバージョン	3026
JSON ポリシードキュメント	3026
詳細はこちら	3027

LexChannelPolicy	3027
このポリシーを使用すると	3027
ポリシーの詳細	3027
ポリシーのバージョン	3028
JSON ポリシードキュメント	3028
詳細はこちら	3028
LightsailExportAccess	3028
このポリシーを使用すると	3029
ポリシーの詳細	3029
ポリシーのバージョン	3029
JSON ポリシードキュメント	3029
詳細はこちら	3030
MediaConnectGatewayInstanceRolePolicy	3030
このポリシーを使用すると	3030
ポリシーの詳細	3030
ポリシーのバージョン	3031
JSON ポリシードキュメント	3031
詳細はこちら	3031
MediaPackageServiceRolePolicy	3031
このポリシーを使用すると	3032
ポリシーの詳細	3032
ポリシーのバージョン	3032
JSON ポリシードキュメント	3032
詳細はこちら	3033
MemoryDBServiceRolePolicy	3033
このポリシーを使用すると	3033
ポリシーの詳細	3033
ポリシーのバージョン	3033
JSON ポリシードキュメント	3034
詳細はこちら	3035
MigrationHubDMSAccessServiceRolePolicy	3036
このポリシーを使用すると	3036
ポリシーの詳細	3036
ポリシーのバージョン	3036
JSON ポリシードキュメント	3036
詳細はこちら	3037

MigrationHubServiceRolePolicy	3037
このポリシーを使用すると	3038
ポリシーの詳細	3038
ポリシーのバージョン	3038
JSON ポリシードキュメント	3038
詳細はこちら	3039
MigrationHubSMSAccessServiceRolePolicy	3040
このポリシーを使用すると	3040
ポリシーの詳細	3040
ポリシーのバージョン	3040
JSON ポリシードキュメント	3040
詳細はこちら	3041
MonitronServiceRolePolicy	3041
このポリシーを使用すると	3042
ポリシーの詳細	3042
ポリシーのバージョン	3042
JSON ポリシードキュメント	3042
詳細はこちら	3043
NeptuneConsoleFullAccess	3043
このポリシーを使用すると	3043
ポリシーの詳細	3043
ポリシーのバージョン	3043
JSON ポリシードキュメント	3043
詳細はこちら	3049
NeptuneFullAccess	3049
このポリシーを使用すると	3049
ポリシーの詳細	3049
ポリシーのバージョン	3050
JSON ポリシードキュメント	3050
詳細はこちら	3054
NeptuneGraphReadOnlyAccess	3054
このポリシーを使用すると	3054
ポリシーの詳細	3054
ポリシーのバージョン	3054
JSON ポリシードキュメント	3055
詳細はこちら	3056

NeptuneReadOnlyAccess	3056
このポリシーを使用すると	3056
ポリシーの詳細	3056
ポリシーのバージョン	3057
JSON ポリシードキュメント	3057
詳細はこちら	3059
NetworkAdministrator	3059
このポリシーを使用すると	3059
ポリシーの詳細	3060
ポリシーのバージョン	3060
JSON ポリシードキュメント	3060
詳細はこちら	3066
OAMFullAccess	3067
このポリシーを使用すると	3067
ポリシーの詳細	3067
ポリシーのバージョン	3067
JSON ポリシードキュメント	3067
詳細はこちら	3068
OAMReadOnlyAccess	3068
このポリシーを使用すると	3068
ポリシーの詳細	3068
ポリシーのバージョン	3068
JSON ポリシードキュメント	3069
詳細はこちら	3069
OpensearchIngestionSelfManagedVpcePolicy	3069
このポリシーを使用すると	3069
ポリシーの詳細	3069
ポリシーのバージョン	3070
JSON ポリシードキュメント	3070
詳細はこちら	3071
PartnerCentralAccountManagementUserRoleAssociation	3071
このポリシーを使用すると	3071
ポリシーの詳細	3071
ポリシーのバージョン	3071
JSON ポリシードキュメント	3072
詳細はこちら	3072

PowerUserAccess	3073
このポリシーを使用すると	3073
ポリシーの詳細	3073
ポリシーのバージョン	3073
JSON ポリシードキュメント	3073
詳細はこちら	3074
QBusinessServiceRolePolicy	3074
このポリシーを使用すると	3074
ポリシーの詳細	3074
ポリシーのバージョン	3075
JSON ポリシードキュメント	3075
詳細はこちら	3076
QuickSightAccessForS3StorageManagementAnalyticsReadOnly	3077
このポリシーを使用すると	3077
ポリシーの詳細	3077
ポリシーのバージョン	3077
JSON ポリシードキュメント	3077
詳細はこちら	3078
RDSCloudHsmAuthorizationRole	3078
このポリシーを使用すると	3078
ポリシーの詳細	3078
ポリシーのバージョン	3079
JSON ポリシードキュメント	3079
詳細はこちら	3079
ReadOnlyAccess	3079
このポリシーを使用すると	3080
ポリシーの詳細	3080
ポリシーのバージョン	3080
JSON ポリシードキュメント	3080
詳細はこちら	3130
ResourceGroupsandTagEditorFullAccess	3130
このポリシーを使用すると	3130
ポリシーの詳細	3130
ポリシーのバージョン	3130
JSON ポリシードキュメント	3130
詳細はこちら	3131

ResourceGroupsandTagEditorReadOnlyAccess	3131
このポリシーを使用すると	3131
ポリシーの詳細	3132
ポリシーのバージョン	3132
JSON ポリシードキュメント	3132
詳細はこちら	3133
ResourceGroupsServiceRolePolicy	3133
このポリシーを使用すると	3133
ポリシーの詳細	3133
ポリシーのバージョン	3133
JSON ポリシードキュメント	3134
詳細はこちら	3134
ROSAAmazonEBSCSIDriverOperatorPolicy	3134
このポリシーを使用すると	3134
ポリシーの詳細	3134
ポリシーのバージョン	3135
JSON ポリシードキュメント	3135
詳細はこちら	3138
ROSACloudNetworkConfigOperatorPolicy	3138
このポリシーを使用すると	3138
ポリシーの詳細	3138
ポリシーのバージョン	3139
JSON ポリシードキュメント	3139
詳細はこちら	3140
ROSAControlPlaneOperatorPolicy	3140
このポリシーを使用すると	3140
ポリシーの詳細	3140
ポリシーのバージョン	3140
JSON ポリシードキュメント	3141
詳細はこちら	3145
ROSAImageRegistryOperatorPolicy	3145
このポリシーを使用すると	3145
ポリシーの詳細	3145
ポリシーのバージョン	3146
JSON ポリシードキュメント	3146
詳細はこちら	3147

ROSAIngressOperatorPolicy	3147
このポリシーを使用すると	3148
ポリシーの詳細	3148
ポリシーのバージョン	3148
JSON ポリシードキュメント	3148
詳細はこちら	3149
ROSAInstallerPolicy	3149
このポリシーを使用すると	3149
ポリシーの詳細	3149
ポリシーのバージョン	3150
JSON ポリシードキュメント	3150
詳細はこちら	3158
ROSAKMSProviderPolicy	3158
このポリシーを使用すると	3158
ポリシーの詳細	3158
ポリシーのバージョン	3158
JSON ポリシードキュメント	3158
詳細はこちら	3159
ROSAKubeControllerPolicy	3159
このポリシーを使用すると	3159
ポリシーの詳細	3160
ポリシーのバージョン	3160
JSON ポリシードキュメント	3160
詳細はこちら	3164
ROSAManageSubscription	3165
このポリシーを使用すると	3165
ポリシーの詳細	3165
ポリシーのバージョン	3165
JSON ポリシードキュメント	3165
詳細はこちら	3166
ROSANodePoolManagementPolicy	3166
このポリシーを使用すると	3166
ポリシーの詳細	3166
ポリシーのバージョン	3167
JSON ポリシードキュメント	3167
詳細はこちら	3172

ROSASRESupportPolicy	3173
このポリシーを使用すると	3173
ポリシーの詳細	3173
ポリシーのバージョン	3173
JSON ポリシードキュメント	3173
詳細はこちら	3178
ROSAWorkerInstancePolicy	3178
このポリシーを使用すると	3179
ポリシーの詳細	3179
ポリシーのバージョン	3179
JSON ポリシードキュメント	3179
詳細はこちら	3179
Route53RecoveryReadinessServiceRolePolicy	3180
このポリシーを使用すると	3180
ポリシーの詳細	3180
ポリシーのバージョン	3180
JSON ポリシードキュメント	3180
詳細はこちら	3184
Route53ResolverServiceRolePolicy	3184
このポリシーを使用すると	3184
ポリシーの詳細	3184
ポリシーのバージョン	3185
JSON ポリシードキュメント	3185
詳細はこちら	3185
S3StorageLensServiceRolePolicy	3185
このポリシーを使用すると	3186
ポリシーの詳細	3186
ポリシーのバージョン	3186
JSON ポリシードキュメント	3186
詳細はこちら	3187
SecretsManagerReadWrite	3187
このポリシーを使用すると	3187
ポリシーの詳細	3187
ポリシーのバージョン	3187
JSON ポリシードキュメント	3188
詳細はこちら	3189

SecurityAudit	3189
このポリシーを使用すると	3190
ポリシーの詳細	3190
ポリシーのバージョン	3190
JSON ポリシードキュメント	3190
詳細はこちら	3207
SecurityLakeServiceLinkedRole	3207
このポリシーを使用すると	3208
ポリシーの詳細	3208
ポリシーのバージョン	3208
JSON ポリシードキュメント	3208
詳細はこちら	3211
ServerMigration_ServiceRole	3211
このポリシーを使用すると	3211
ポリシーの詳細	3211
ポリシーのバージョン	3212
JSON ポリシードキュメント	3212
詳細はこちら	3216
ServerMigrationConnector	3217
このポリシーを使用すると	3217
ポリシーの詳細	3217
ポリシーのバージョン	3217
JSON ポリシードキュメント	3217
詳細はこちら	3219
ServerMigrationServiceConsoleFullAccess	3219
このポリシーを使用すると	3219
ポリシーの詳細	3219
ポリシーのバージョン	3220
JSON ポリシードキュメント	3220
詳細はこちら	3221
ServerMigrationServiceLaunchRole	3222
このポリシーを使用すると	3222
ポリシーの詳細	3222
ポリシーのバージョン	3222
JSON ポリシードキュメント	3222
詳細はこちら	3225

ServerMigrationServiceRoleForInstanceValidation	3225
このポリシーを使用すると	3225
ポリシーの詳細	3225
ポリシーのバージョン	3226
JSON ポリシードキュメント	3226
詳細はこちら	3226
ServiceQuotasFullAccess	3227
このポリシーを使用すると	3227
ポリシーの詳細	3227
ポリシーのバージョン	3227
JSON ポリシードキュメント	3227
詳細はこちら	3229
ServiceQuotasReadOnlyAccess	3229
このポリシーを使用すると	3229
ポリシーの詳細	3229
ポリシーのバージョン	3230
JSON ポリシードキュメント	3230
詳細はこちら	3231
ServiceQuotasServiceRolePolicy	3231
このポリシーを使用すると	3231
ポリシーの詳細	3231
ポリシーのバージョン	3232
JSON ポリシードキュメント	3232
詳細はこちら	3232
SimpleWorkflowFullAccess	3232
このポリシーを使用すると	3232
ポリシーの詳細	3233
ポリシーのバージョン	3233
JSON ポリシードキュメント	3233
詳細はこちら	3233
SplitCostAllocationDataServiceRolePolicy	3234
このポリシーを使用すると	3234
ポリシーの詳細	3234
ポリシーのバージョン	3234
JSON ポリシードキュメント	3234
詳細はこちら	3235

SupportUser	3235
このポリシーを使用すると	3235
ポリシーの詳細	3235
ポリシーのバージョン	3236
JSON ポリシードキュメント	3236
詳細はこちら	3241
SystemAdministrator	3241
このポリシーを使用すると	3241
ポリシーの詳細	3241
ポリシーのバージョン	3241
JSON ポリシードキュメント	3242
詳細はこちら	3248
TranslateFullAccess	3248
このポリシーを使用すると	3248
ポリシーの詳細	3248
ポリシーのバージョン	3248
JSON ポリシードキュメント	3248
詳細はこちら	3249
TranslateReadOnly	3249
このポリシーを使用すると	3249
ポリシーの詳細	3249
ポリシーのバージョン	3250
JSON ポリシードキュメント	3250
詳細はこちら	3250
ViewOnlyAccess	3251
このポリシーを使用すると	3251
ポリシーの詳細	3251
ポリシーのバージョン	3251
JSON ポリシードキュメント	3251
詳細はこちら	3260
VMImportExportRoleForAWSConnector	3260
このポリシーを使用すると	3260
ポリシーの詳細	3260
ポリシーのバージョン	3261
JSON ポリシードキュメント	3261
詳細はこちら	3262

VPCLatticeFullAccess	3262
このポリシーを使用すると	3262
ポリシーの詳細	3262
ポリシーのバージョン	3262
JSON ポリシードキュメント	3262
詳細はこちら	3264
VPCLatticeReadOnlyAccess	3265
このポリシーを使用すると	3265
ポリシーの詳細	3265
ポリシーのバージョン	3265
JSON ポリシードキュメント	3265
詳細はこちら	3266
VPCLatticeServicesInvokeAccess	3266
このポリシーを使用すると	3266
ポリシーの詳細	3266
ポリシーのバージョン	3267
JSON ポリシードキュメント	3267
詳細はこちら	3267
WAFLoggingServiceRolePolicy	3267
このポリシーを使用すると	3268
ポリシーの詳細	3268
ポリシーのバージョン	3268
JSON ポリシードキュメント	3268
詳細はこちら	3269
WAFRegionalLoggingServiceRolePolicy	3269
このポリシーを使用すると	3269
ポリシーの詳細	3269
ポリシーのバージョン	3269
JSON ポリシードキュメント	3269
詳細はこちら	3270
WAFV2LoggingServiceRolePolicy	3270
このポリシーを使用すると	3270
ポリシーの詳細	3270
ポリシーのバージョン	3271
JSON ポリシードキュメント	3271
詳細はこちら	3271

WellArchitectedConsoleFullAccess	3272
このポリシーを使用すると	3272
ポリシーの詳細	3272
ポリシーのバージョン	3272
JSON ポリシードキュメント	3272
詳細はこちら	3273
WellArchitectedConsoleReadOnlyAccess	3273
このポリシーを使用すると	3273
ポリシーの詳細	3273
ポリシーのバージョン	3273
JSON ポリシードキュメント	3274
詳細はこちら	3274
WorkLinkServiceRolePolicy	3274
このポリシーを使用すると	3274
ポリシーの詳細	3274
ポリシーのバージョン	3275
JSON ポリシードキュメント	3275
詳細はこちら	3275
.....	mmmcclxxvii

AWS マネージドポリシーとは何ですか？

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されています。これにより、自身でポリシーを記述するよりも簡単に、ユーザー、グループ、ロールに許可を割り当てることができます。

AWS マネージドポリシーは、すべての AWS のユーザーが使用できるため、特定のユースケースに対して最小特権のアクセス許可が付与されない場合があることに留意してください。ユースケース別に [カスタマーマネージドポリシー](#) を定義することで、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS サービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の [「AWS マネージドポリシー」](#) を参照してください。

ポリシーリファレンスページについて

各ポリシーリファレンスページには、以下の情報が含まれています。

- このポリシーを使用すると — ユーザー、グループ、ロールにポリシーをアタッチできるかどうか
- ポリシーの詳細
 - タイプ — AWS マネージドポリシーのタイプ
 - AWS managed policy — 標準 AWS マネージドポリシー
 - Job function policy — 一般的な業界職務に沿ったポリシー
 - Service-linked role policy — ユーザーに代わって [the section called “AmazonRDSPreviewServiceRolePolicy”](#) のようなアクションを実行することをサービスに許可する、サービスリンクロールにアタッチするポリシー
 - Service role policy — [the section called “AWSControlTowerServiceRolePolicy”](#) のようなサービスロールと連携するように設計されたポリシー
 - 作成日時 — ポリシーが最初に作成された日時
 - 編集日時 — このバージョンのポリシーが編集された日時

- ARN — ポリシーの Amazon リソースネーム
- ポリシーのバージョン — ポリシーによって付与された許可バージョン
- JSON ポリシードキュメント — ポリシー JSON
- 詳細 — AWS マネージドポリシーに関連するドキュメントへのリンク

非推奨の AWS マネージドポリシー

AWS は、AWS マネージドポリシーを定期的に更新します。ほとんどの場合、アクセス許可をポリシーに追加します。これは、新しいサービスや機能をリリースしたときに行われます。AWS マネージドポリシーのセキュリティを向上させるために、ポリシーの範囲を縮小することがあります。ポリシーからアクセス許可を削除すると、ポリシーを非推奨の状態に設定し、新しいポリシーを利用できるようにします。AWS がサービスまたは機能を廃止すると、その機能の AWS マネージドポリシーも廃止されます。

使用しているポリシーが廃止されたというメール通知を受け取った場合は、直ちに対応することをお勧めします。ポリシーの変更を特定し、ワークフローを更新してください。AWS が交換ポリシーを提供する場合、影響を受けるすべてのアイデンティティ (ユーザー、グループ、およびロール) にそのポリシーをアタッチした後、それらのアイデンティティから廃止されたポリシーをデタッチします。

非推奨のポリシーには以下のような特徴があります。

- このガイドからは削除されています。
- アクセス許可は、現在アタッチされているすべてのアイデンティティに対して引き続き機能します。
- ポリシーがアイデンティティにアタッチされているアカウントでは、IAM コンソールの [Policies] リストに警告アイコンと共に表示されます。
- 新しいアイデンティティにはアタッチできません。現在のアイデンティティからポリシーをデタッチした場合、再アタッチすることはできません。
- 現在のすべてのエンティティからポリシーをデタッチしたら、そのポリシーは表示されなくなります。

AWS マネージドポリシー

AWS マネージドポリシー

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

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

- [AmazonCodeGuruSecurityFullAccess](#)
- [AmazonCodeGuruSecurityScanAccess](#)
- [AmazonCognitoDeveloperAuthenticatedIdentities](#)
- [AmazonCognitoIdpEmailServiceRolePolicy](#)
- [AmazonCognitoIdpServiceRolePolicy](#)
- [AmazonCognitoPowerUser](#)
- [AmazonCognitoReadOnly](#)
- [AmazonCognitoUnAuthedIdentitiesSessionPolicy](#)
- [AmazonCognitoUnauthenticatedIdentities](#)
- [AmazonConnect_FullAccess](#)
- [AmazonConnectCampaignsServiceLinkedRolePolicy](#)
- [AmazonConnectReadOnlyAccess](#)
- [AmazonConnectServiceLinkedRolePolicy](#)
- [AmazonConnectSynchronizationServiceRolePolicy](#)
- [AmazonConnectVoiceIDFullAccess](#)
- [AmazonDataZoneDomainExecutionRolePolicy](#)
- [AmazonDataZoneEnvironmentRolePermissionsBoundary](#)
- [AmazonDataZoneFullAccess](#)
- [AmazonDataZoneFullUserAccess](#)
- [AmazonDataZoneGlueManageAccessRolePolicy](#)
- [AmazonDataZonePortalFullAccessPolicy](#)
- [AmazonDataZonePreviewConsoleFullAccess](#)
- [AmazonDataZoneProjectDeploymentPermissionsBoundary](#)
- [AmazonDataZoneProjectRolePermissionsBoundary](#)
- [AmazonDataZoneRedshiftGlueProvisioningPolicy](#)
- [AmazonDataZoneRedshiftManageAccessRolePolicy](#)
- [AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary](#)
- [AmazonDataZoneSageMakerManageAccessRolePolicy](#)
- [AmazonDataZoneSageMakerProvisioningRolePolicy](#)

- [AmazonDetectiveFullAccess](#)
- [AmazonDetectiveInvestigatorAccess](#)
- [AmazonDetectiveMemberAccess](#)
- [AmazonDetectiveOrganizationsAccess](#)
- [AmazonDetectiveServiceLinkedRolePolicy](#)
- [AmazonDevOpsGuruConsoleFullAccess](#)
- [AmazonDevOpsGuruFullAccess](#)
- [AmazonDevOpsGuruOrganizationsAccess](#)
- [AmazonDevOpsGuruReadOnlyAccess](#)
- [AmazonDevOpsGuruServiceRolePolicy](#)
- [AmazonDMSCloudWatchLogsRole](#)
- [AmazonDMSRedshiftS3Role](#)
- [AmazonDMSVPCManagementRole](#)
- [AmazonDocDB-ElasticServiceRolePolicy](#)
- [AmazonDocDBConsoleFullAccess](#)
- [AmazonDocDBElasticFullAccess](#)
- [AmazonDocDBElasticReadOnlyAccess](#)
- [AmazonDocDBFullAccess](#)
- [AmazonDocDBReadOnlyAccess](#)
- [AmazonDRSVPCManagement](#)
- [AmazonDynamoDBFullAccess](#)
- [AmazonDynamoDBFullAccesswithDataPipeline](#)
- [AmazonDynamoDBReadOnlyAccess](#)
- [AmazonEBSCSIDriverPolicy](#)
- [AmazonEC2ContainerRegistryFullAccess](#)
- [AmazonEC2ContainerRegistryPowerUser](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- [AmazonEC2ContainerServiceAutoscaleRole](#)
- [AmazonEC2ContainerServiceEventsRole](#)

- [AmazonEC2ContainerServiceforEC2Role](#)
- [AmazonEC2ContainerServiceRole](#)
- [AmazonEC2FullAccess](#)
- [AmazonEC2ReadOnlyAccess](#)
- [AmazonEC2RoleforAWSCodeDeploy](#)
- [AmazonEC2RoleforAWSCodeDeployLimited](#)
- [AmazonEC2RoleforDataPipelineRole](#)
- [AmazonEC2RoleforSSM](#)
- [AmazonEC2RolePolicyForLaunchWizard](#)
- [AmazonEC2SpotFleetAutoscaleRole](#)
- [AmazonEC2SpotFleetTaggingRole](#)
- [AmazonECS_FullAccess](#)
- [AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity](#)
- [AmazonECSInfrastructureRolePolicyForVolumes](#)
- [AmazonECSServiceRolePolicy](#)
- [AmazonECSTaskExecutionRolePolicy](#)
- [AmazonEFSCSIDriverPolicy](#)
- [AmazonEKS_CNI_Policy](#)
- [AmazonEKSClusterPolicy](#)
- [AmazonEKSConnectorserviceRolePolicy](#)
- [AmazonEKSFargatePodExecutionRolePolicy](#)
- [AmazonEKSFargateServiceRolePolicy](#)
- [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](#)
- [AmazonOpenSearchDirectQueryGlueCreateAccess](#)
- [AmazonOpenSearchIngestionFullAccess](#)
- [AmazonOpenSearchIngestionReadOnlyAccess](#)
- [AmazonOpenSearchIngestionServiceRolePolicy](#)
- [AmazonOpenSearchServerlessServiceRolePolicy](#)
- [AmazonOpenSearchServiceCognitoAccess](#)
- [AmazonOpenSearchServiceFullAccess](#)
- [AmazonOpenSearchServiceReadOnlyAccess](#)
- [AmazonOpenSearchServiceRolePolicy](#)
- [AmazonPersonalizeFullAccess](#)
- [AmazonPollyFullAccess](#)
- [AmazonPollyReadOnlyAccess](#)
- [AmazonPrometheusConsoleFullAccess](#)
- [AmazonPrometheusFullAccess](#)
- [AmazonPrometheusQueryAccess](#)
- [AmazonPrometheusRemoteWriteAccess](#)
- [AmazonPrometheusScraperServiceRolePolicy](#)
- [AmazonQFullAccess](#)
- [AmazonQLDBConsoleFullAccess](#)
- [AmazonQLDBFullAccess](#)

- [AmazonQLDBReadOnly](#)
- [AmazonRDSBetaServiceRolePolicy](#)
- [AmazonRDSCustomInstanceProfileRolePolicy](#)
- [AmazonRDSCustomPreviewServiceRolePolicy](#)
- [AmazonRDSCustomServiceRolePolicy](#)
- [AmazonRDSDataFullAccess](#)
- [AmazonRDSDirectoryServiceAccess](#)
- [AmazonRDSEnhancedMonitoringRole](#)
- [AmazonRDSFullAccess](#)
- [AmazonRDSPerformanceInsightsFullAccess](#)
- [AmazonRDSPerformanceInsightsReadOnly](#)
- [AmazonRDSPreviewServiceRolePolicy](#)
- [AmazonRDSReadOnlyAccess](#)
- [AmazonRDSServiceRolePolicy](#)
- [AmazonRedshiftAllCommandsFullAccess](#)
- [AmazonRedshiftDataFullAccess](#)
- [AmazonRedshiftFullAccess](#)
- [AmazonRedshiftQueryEditor](#)
- [AmazonRedshiftQueryEditorV2FullAccess](#)
- [AmazonRedshiftQueryEditorV2NoSharing](#)
- [AmazonRedshiftQueryEditorV2ReadSharing](#)
- [AmazonRedshiftQueryEditorV2ReadWriteSharing](#)
- [AmazonRedshiftReadOnlyAccess](#)
- [AmazonRedshiftServiceLinkedRolePolicy](#)
- [AmazonRekognitionCustomLabelsFullAccess](#)
- [AmazonRekognitionFullAccess](#)
- [AmazonRekognitionReadOnlyAccess](#)
- [AmazonRekognitionServiceRole](#)
- [AmazonRoute53AutoNamingFullAccess](#)

- [AmazonRoute53AutoNamingReadOnlyAccess](#)
- [AmazonRoute53AutoNamingRegistrantAccess](#)
- [AmazonRoute53DomainsFullAccess](#)
- [AmazonRoute53DomainsReadOnlyAccess](#)
- [AmazonRoute53FullAccess](#)
- [AmazonRoute53ProfilesFullAccess](#)
- [AmazonRoute53ProfilesReadOnlyAccess](#)
- [AmazonRoute53ReadOnlyAccess](#)
- [AmazonRoute53RecoveryClusterFullAccess](#)
- [AmazonRoute53RecoveryClusterReadOnlyAccess](#)
- [AmazonRoute53RecoveryControlConfigFullAccess](#)
- [AmazonRoute53RecoveryControlConfigReadOnlyAccess](#)
- [AmazonRoute53RecoveryReadinessFullAccess](#)
- [AmazonRoute53RecoveryReadinessReadOnlyAccess](#)
- [AmazonRoute53ResolverFullAccess](#)
- [AmazonRoute53ResolverReadOnlyAccess](#)
- [AmazonS3FullAccess](#)
- [AmazonS3ObjectLambdaExecutionRolePolicy](#)
- [AmazonS3OutpostsFullAccess](#)
- [AmazonS3OutpostsReadOnlyAccess](#)
- [AmazonS3ReadOnlyAccess](#)
- [AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy](#)
- [AmazonSageMakerCanvasAIServicesAccess](#)
- [AmazonSageMakerCanvasBedrockAccess](#)
- [AmazonSageMakerCanvasDataPrepFullAccess](#)
- [AmazonSageMakerCanvasDirectDeployAccess](#)
- [AmazonSageMakerCanvasForecastAccess](#)
- [AmazonSageMakerCanvasFullAccess](#)
- [AmazonSageMakerClusterInstanceRolePolicy](#)

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

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

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

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

- [AWSApplicationMigrationAgentInstallationPolicy](#)
- [AWSApplicationMigrationAgentPolicy](#)
- [AWSApplicationMigrationAgentPolicy_v2](#)
- [AWSApplicationMigrationConversionServerPolicy](#)
- [AWSApplicationMigrationEC2Access](#)
- [AWSApplicationMigrationFullAccess](#)
- [AWSApplicationMigrationMGHAccess](#)
- [AWSApplicationMigrationReadOnlyAccess](#)
- [AWSApplicationMigrationReplicationServerPolicy](#)
- [AWSApplicationMigrationServiceEc2InstancePolicy](#)
- [AWSApplicationMigrationServiceRolePolicy](#)
- [AWSApplicationMigrationSSMAccess](#)
- [AWSApplicationMigrationVCenterClientPolicy](#)
- [AWSAppMeshEnvoyAccess](#)
- [AWSAppMeshFullAccess](#)
- [AWSAppMeshPreviewEnvoyAccess](#)
- [AWSAppMeshPreviewServiceRolePolicy](#)
- [AWSAppMeshReadOnly](#)
- [AWSAppMeshServiceRolePolicy](#)
- [AWSAppRunnerFullAccess](#)
- [AWSAppRunnerReadOnlyAccess](#)
- [AWSAppRunnerServicePolicyForECRAccess](#)
- [AWSAppSyncAdministrator](#)
- [AWSAppSyncInvokeFullAccess](#)
- [AWSAppSyncPushToCloudWatchLogs](#)
- [AWSAppSyncSchemaAuthor](#)
- [AWSAppSyncServiceRolePolicy](#)
- [AWSArtifactAccountSync](#)
- [AWSArtifactReportsReadOnlyAccess](#)

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

- [AWSBugBustServiceRolePolicy](#)
- [AWSCertificateManagerFullAccess](#)
- [AWSCertificateManagerPrivateCAAuditor](#)
- [AWSCertificateManagerPrivateCAFullAccess](#)
- [AWSCertificateManagerPrivateCAPrivilegedUser](#)
- [AWSCertificateManagerPrivateCARedOnly](#)
- [AWSCertificateManagerPrivateCAUser](#)
- [AWSCertificateManagerReadOnly](#)
- [AWSChatbotServiceLinkedRolePolicy](#)
- [AWSCleanRoomsFullAccess](#)
- [AWSCleanRoomsFullAccessNoQuerying](#)
- [AWSCleanRoomsMLFullAccess](#)
- [AWSCleanRoomsMLReadOnlyAccess](#)
- [AWSCleanRoomsReadOnlyAccess](#)
- [AWSCloud9Administrator](#)
- [AWSCloud9EnvironmentMember](#)
- [AWSCloud9ServiceRolePolicy](#)
- [AWSCloud9SSMInstanceProfile](#)
- [AWSCloud9User](#)
- [AWSCloudFormationFullAccess](#)
- [AWSCloudFormationReadOnlyAccess](#)
- [AWSCloudFrontLogger](#)
- [AWSCloudHSMFullAccess](#)
- [AWSCloudHSMReadOnlyAccess](#)
- [AWSCloudHSMRole](#)
- [AWSCloudMapDiscoverInstanceAccess](#)
- [AWSCloudMapFullAccess](#)
- [AWSCloudMapReadOnlyAccess](#)
- [AWSCloudMapRegisterInstanceAccess](#)

- [AWSCloudShellFullAccess](#)
- [AWSCloudTrail_FullAccess](#)
- [AWSCloudTrail_ReadOnlyAccess](#)
- [AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy](#)
- [AWSCodeArtifactAdminAccess](#)
- [AWSCodeArtifactReadOnlyAccess](#)
- [AWSCodeBuildAdminAccess](#)
- [AWSCodeBuildDeveloperAccess](#)
- [AWSCodeBuildReadOnlyAccess](#)
- [AWSCodeCommitFullAccess](#)
- [AWSCodeCommitPowerUser](#)
- [AWSCodeCommitReadOnly](#)
- [AWSCodeDeployDeployerAccess](#)
- [AWSCodeDeployFullAccess](#)
- [AWSCodeDeployReadOnlyAccess](#)
- [AWSCodeDeployRole](#)
- [AWSCodeDeployRoleForCloudFormation](#)
- [AWSCodeDeployRoleForECS](#)
- [AWSCodeDeployRoleForECSLimited](#)
- [AWSCodeDeployRoleForLambda](#)
- [AWSCodeDeployRoleForLambdaLimited](#)
- [AWSCodePipeline_FullAccess](#)
- [AWSCodePipeline_ReadOnlyAccess](#)
- [AWSCodePipelineApproverAccess](#)
- [AWSCodePipelineCustomActionAccess](#)
- [AWSCodeStarFullAccess](#)
- [AWSCodeStarNotificationsServiceRolePolicy](#)
- [AWSCodeStarServiceRole](#)
- [AWSCompromisedKeyQuarantine](#)

- [AWSCompromisedKeyQuarantineV2](#)
- [AWSConfigMultiAccountSetupPolicy](#)
- [AWSConfigRemediationServiceRolePolicy](#)
- [AWSConfigRoleForOrganizations](#)
- [AWSConfigRulesExecutionRole](#)
- [AWSConfigServiceRolePolicy](#)
- [AWSConfigUserAccess](#)
- [AWSConnector](#)
- [AWSControlTowerAccountServiceRolePolicy](#)
- [AWSControlTowerServiceRolePolicy](#)
- [AWSCostAndUsageReportAutomationPolicy](#)
- [AWSDataExchangeFullAccess](#)
- [AWSDataExchangeProviderFullAccess](#)
- [AWSDataExchangeReadOnly](#)
- [AWSDataExchangeSubscriberFullAccess](#)
- [AWSDataLifecycleManagerServiceRole](#)
- [AWSDataLifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDataLifecycleManagerSSMFullAccess](#)
- [AWSDataPipeline_FullAccess](#)
- [AWSDataPipeline_PowerUser](#)
- [AWSDataSyncDiscoveryServiceRolePolicy](#)
- [AWSDataSyncFullAccess](#)
- [AWSDataSyncReadOnlyAccess](#)
- [AWSDeadlineCloud-FleetWorker](#)
- [AWSDeadlineCloud-UserAccessFarms](#)
- [AWSDeadlineCloud-UserAccessFleets](#)
- [AWSDeadlineCloud-UserAccessJobs](#)
- [AWSDeadlineCloud-UserAccessQueues](#)
- [AWSDeadlineCloud-WorkerHost](#)

- [AWSDeepLensLambdaFunctionAccessPolicy](#)
- [AWSDeepLensServiceRolePolicy](#)
- [AWSDeepRacerAccountAdminAccess](#)
- [AWSDeepRacerCloudFormationAccessPolicy](#)
- [AWSDeepRacerDefaultMultiUserAccess](#)
- [AWSDeepRacerFullAccess](#)
- [AWSDeepRacerRoboMakerAccessPolicy](#)
- [AWSDeepRacerServiceRolePolicy](#)
- [AWSDenyAll](#)
- [AWSDeviceFarmFullAccess](#)
- [AWSDeviceFarmServiceRolePolicy](#)
- [AWSDeviceFarmTestGridServiceRolePolicy](#)
- [AWSDirectConnectFullAccess](#)
- [AWSDirectConnectReadOnlyAccess](#)
- [AWSDirectConnectServiceRolePolicy](#)
- [AWSDirectoryServiceFullAccess](#)
- [AWSDirectoryServiceReadOnlyAccess](#)
- [AWSDiscoveryContinuousExportFirehosePolicy](#)
- [AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWSDMSServerlessServiceRolePolicy](#)
- [AWSEC2CapacityReservationFleetRolePolicy](#)
- [AWSEC2FleetServiceRolePolicy](#)
- [AWSEC2SpotFleetServiceRolePolicy](#)
- [AWSEC2SpotServiceRolePolicy](#)
- [AWSEC2VssSnapshotPolicy](#)
- [AWSECRPullThroughCache_ServiceRolePolicy](#)
- [AWSElasticBeanstalkCustomPlatformforEC2Role](#)
- [AWSElasticBeanstalkEnhancedHealth](#)
- [AWSElasticBeanstalkMaintenance](#)

- [AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy](#)
- [AWSElasticBeanstalkManagedUpdatesServiceRolePolicy](#)
- [AWSElasticBeanstalkMulticontainerDocker](#)
- [AWSElasticBeanstalkReadOnly](#)
- [AWSElasticBeanstalkRoleCore](#)
- [AWSElasticBeanstalkRoleCWL](#)
- [AWSElasticBeanstalkRoleECS](#)
- [AWSElasticBeanstalkRoleRDS](#)
- [AWSElasticBeanstalkRoleSNS](#)
- [AWSElasticBeanstalkRoleWorkerTier](#)
- [AWSElasticBeanstalkService](#)
- [AWSElasticBeanstalkServiceRolePolicy](#)
- [AWSElasticBeanstalkWebTier](#)
- [AWSElasticBeanstalkWorkerTier](#)
- [AWSElasticDisasterRecoveryAgentInstallationPolicy](#)
- [AWSElasticDisasterRecoveryAgentPolicy](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess](#)
- [AWSElasticDisasterRecoveryConsoleFullAccess_v2](#)
- [AWSElasticDisasterRecoveryConversionServerPolicy](#)
- [AWSElasticDisasterRecoveryCrossAccountReplicationPolicy](#)
- [AWSElasticDisasterRecoveryEc2InstancePolicy](#)
- [AWSElasticDisasterRecoveryFailbackInstallationPolicy](#)
- [AWSElasticDisasterRecoveryFailbackPolicy](#)
- [AWSElasticDisasterRecoveryLaunchActionsPolicy](#)
- [AWSElasticDisasterRecoveryNetworkReplicationPolicy](#)
- [AWSElasticDisasterRecoveryReadOnlyAccess](#)
- [AWSElasticDisasterRecoveryRecoveryInstancePolicy](#)
- [AWSElasticDisasterRecoveryReplicationServerPolicy](#)
- [AWSElasticDisasterRecoveryServiceRolePolicy](#)
- [AWSElasticDisasterRecoveryStagingAccountPolicy](#)

- [AWSElasticDisasterRecoveryStagingAccountPolicy_v2](#)
- [AWSElasticLoadBalancingClassicServiceRolePolicy](#)
- [AWSElasticLoadBalancingServiceRolePolicy](#)
- [AWSElementalMediaConvertFullAccess](#)
- [AWSElementalMediaConvertReadOnly](#)
- [AWSElementalMediaLiveFullAccess](#)
- [AWSElementalMediaLiveReadOnly](#)
- [AWSElementalMediaPackageFullAccess](#)
- [AWSElementalMediaPackageReadOnly](#)
- [AWSElementalMediaPackageV2FullAccess](#)
- [AWSElementalMediaPackageV2ReadOnly](#)
- [AWSElementalMediaStoreFullAccess](#)
- [AWSElementalMediaStoreReadOnly](#)
- [AWSElementalMediaTailorFullAccess](#)
- [AWSElementalMediaTailorReadOnly](#)
- [AWSEnhancedClassicNetworkingMangementPolicy](#)
- [AWSEntityResolutionConsoleFullAccess](#)
- [AWSEntityResolutionConsoleReadOnlyAccess](#)
- [AWSFaultInjectionSimulatorEC2Access](#)
- [AWSFaultInjectionSimulatorECSAccess](#)
- [AWSFaultInjectionSimulatorEKSAccess](#)
- [AWSFaultInjectionSimulatorNetworkAccess](#)
- [AWSFaultInjectionSimulatorRDSAccess](#)
- [AWSFaultInjectionSimulatorSSMAccess](#)
- [AWSFinSpaceServiceRolePolicy](#)
- [AWSFMAdminFullAccess](#)
- [AWSFMAdminReadOnlyAccess](#)
- [AWSFMMemberReadOnlyAccess](#)
- [AWSForWordPressPluginPolicy](#)
- [AWSGitSyncServiceRolePolicy](#)

- [AWSGlobalAcceleratorSLRPolicy](#)
- [AWSGlueConsoleFullAccess](#)
- [AWSGlueConsoleSageMakerNotebookFullAccess](#)
- [AwsGlueDataBrewFullAccessPolicy](#)
- [AWSGlueDataBrewServiceRole](#)
- [AWSGlueSchemaRegistryFullAccess](#)
- [AWSGlueSchemaRegistryReadOnlyAccess](#)
- [AWSGlueServiceNotebookRole](#)
- [AWSGlueServiceRole](#)
- [AwsGlueSessionUserRestrictedNotebookPolicy](#)
- [AwsGlueSessionUserRestrictedNotebookServiceRole](#)
- [AwsGlueSessionUserRestrictedPolicy](#)
- [AwsGlueSessionUserRestrictedServiceRole](#)
- [AWSGrafanaAccountAdministrator](#)
- [AWSGrafanaConsoleReadOnlyAccess](#)
- [AWSGrafanaWorkspacePermissionManagement](#)
- [AWSGrafanaWorkspacePermissionManagementV2](#)
- [AWSGreengrassFullAccess](#)
- [AWSGreengrassReadOnlyAccess](#)
- [AWSGreengrassResourceAccessRolePolicy](#)
- [AWSGroundStationAgentInstancePolicy](#)
- [AWSHealth_EventProcessorServiceRolePolicy](#)
- [AWSHealthFullAccess](#)
- [AWSHealthImagingFullAccess](#)
- [AWSHealthImagingReadOnlyAccess](#)
- [AWSIAMIdentityCenterAllowListForIdentityContext](#)
- [AWSIdentitySyncFullAccess](#)
- [AWSIdentitySyncReadOnlyAccess](#)
- [AWSImageBuilderFullAccess](#)
- [AWSImageBuilderReadOnlyAccess](#)

- [AWSImportExportFullAccess](#)
- [AWSImportExportReadOnlyAccess](#)
- [AWSIncidentManagerIncidentAccessServiceRolePolicy](#)
- [AWSIncidentManagerResolverAccess](#)
- [AWSIncidentManagerServiceRolePolicy](#)
- [AWSIoT1ClickFullAccess](#)
- [AWSIoT1ClickReadOnlyAccess](#)
- [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](#)
- [AWSPrivateCAAuditor](#)
- [AWSPrivateCAFullAccess](#)
- [AWSPrivateCAPrivilegedUser](#)
- [AWSPrivateCARedOnly](#)
- [AWSPrivateCAUser](#)
- [AWSPrivateMarketplaceAdminFullAccess](#)
- [AWSPrivateMarketplaceRequests](#)
- [AWSPrivateNetworksServiceRolePolicy](#)
- [AWSProtonCodeBuildProvisioningBasicAccess](#)
- [AWSProtonCodeBuildProvisioningServiceRolePolicy](#)

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

- [AWSResourceExplorerServiceRolePolicy](#)
- [AWSResourceGroupsReadOnlyAccess](#)
- [AWSRoboMaker_FullAccess](#)
- [AWSRoboMakerReadOnlyAccess](#)
- [AWSRoboMakerServicePolicy](#)
- [AWSRoboMakerServiceRolePolicy](#)
- [AWSRolesAnywhereServicePolicy](#)
- [AWSS3OnOutpostsServiceRolePolicy](#)
- [AWSSavingsPlansFullAccess](#)
- [AWSSavingsPlansReadOnlyAccess](#)
- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)
- [AWSSecurityHubReadOnlyAccess](#)
- [AWSSecurityHubServiceRolePolicy](#)
- [AWSServiceCatalogAdminFullAccess](#)
- [AWSServiceCatalogAdminReadOnlyAccess](#)
- [AWSServiceCatalogAppRegistryFullAccess](#)
- [AWSServiceCatalogAppRegistryReadOnlyAccess](#)
- [AWSServiceCatalogAppRegistryServiceRolePolicy](#)
- [AWSServiceCatalogEndUserFullAccess](#)
- [AWSServiceCatalogEndUserReadOnlyAccess](#)
- [AWSServiceCatalogOrgsDataSyncServiceRolePolicy](#)
- [AWSServiceCatalogSyncServiceRolePolicy](#)
- [AWSServiceRoleForAmazonEKSNodegroup](#)
- [AWSServiceRoleForAmazonQDeveloper](#)
- [AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy](#)
- [AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy](#)
- [AWSServiceRoleForCodeGuru-Profiler](#)
- [AWSServiceRoleForCodeWhispererPolicy](#)
- [AWSServiceRoleForEC2ScheduledInstances](#)

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

- [AWSSupportAppReadOnlyAccess](#)
- [AWSSupportPlansFullAccess](#)
- [AWSSupportPlansReadOnlyAccess](#)
- [AWSSupportServiceRolePolicy](#)
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)
- [AWSSystemsManagerChangeManagementServicePolicy](#)
- [AWSSystemsManagerForSAPFullAccess](#)
- [AWSSystemsManagerForSAPReadOnlyAccess](#)
- [AWSSystemsManagerOpsDataSyncServiceRolePolicy](#)
- [AWSThinkboxAssetServerPolicy](#)
- [AWSThinkboxAWSPortalAdminPolicy](#)
- [AWSThinkboxAWSPortalGatewayPolicy](#)
- [AWSThinkboxAWSPortalWorkerPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAccessPolicy](#)
- [AWSThinkboxDeadlineResourceTrackerAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginAdminPolicy](#)
- [AWSThinkboxDeadlineSpotEventPluginWorkerPolicy](#)
- [AWSTransferConsoleFullAccess](#)
- [AWSTransferFullAccess](#)
- [AWSTransferLoggingAccess](#)
- [AWSTransferReadOnlyAccess](#)
- [AWSTrustedAdvisorPriorityFullAccess](#)
- [AWSTrustedAdvisorPriorityReadOnlyAccess](#)
- [AWSTrustedAdvisorReportingServiceRolePolicy](#)
- [AWSTrustedAdvisorServiceRolePolicy](#)
- [AWSUserNotificationsServiceLinkedRolePolicy](#)
- [AWSVendorInsightsAssessorFullAccess](#)
- [AWSVendorInsightsAssessorReadOnly](#)
- [AWSVendorInsightsVendorFullAccess](#)
- [AWSVendorInsightsVendorReadOnly](#)

- [AWSVpcLatticeServiceRolePolicy](#)
- [AWSVPCS2SVpnServiceRolePolicy](#)
- [AWSVPCTransitGatewayServiceRolePolicy](#)
- [AWSVPCVerifiedAccessServiceRolePolicy](#)
- [AWSWAFConsoleFullAccess](#)
- [AWSWAFConsoleReadOnlyAccess](#)
- [AWSWAFFullAccess](#)
- [AWSWAFReadOnlyAccess](#)
- [AWSWellArchitectedDiscoveryServiceRolePolicy](#)
- [AWSWellArchitectedOrganizationsServiceRolePolicy](#)
- [AWSWickrFullAccess](#)
- [AWSXrayCrossAccountSharingConfiguration](#)
- [AWSXRayDaemonWriteAccess](#)
- [AWSXrayFullAccess](#)
- [AWSXrayReadOnlyAccess](#)
- [AWSXrayWriteOnlyAccess](#)
- [AWSZonalAutoshiftPracticeRunSLRPolicy](#)
- [BatchServiceRolePolicy](#)
- [Billing](#)
- [CertificateManagerServiceRolePolicy](#)
- [ClientVPNServiceConnectionsRolePolicy](#)
- [ClientVPNServiceRolePolicy](#)
- [CloudFormationStackSetsOrgAdminServiceRolePolicy](#)
- [CloudFormationStackSetsOrgMemberServiceRolePolicy](#)
- [CloudFrontFullAccess](#)
- [CloudFrontReadOnlyAccess](#)
- [CloudHSMServiceRolePolicy](#)
- [CloudSearchFullAccess](#)
- [CloudSearchReadOnlyAccess](#)
- [CloudTrailServiceRolePolicy](#)

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

- [ComprehendMedicalFullAccess](#)
- [ComprehendReadOnly](#)
- [ComputeOptimizerReadOnlyAccess](#)
- [ComputeOptimizerServiceRolePolicy](#)
- [ConfigConformsServiceRolePolicy](#)
- [CostOptimizationHubAdminAccess](#)
- [CostOptimizationHubReadOnlyAccess](#)
- [CostOptimizationHubServiceRolePolicy](#)
- [CustomerProfilesServiceLinkedRolePolicy](#)
- [DatabaseAdministrator](#)
- [DataScientist](#)
- [DAXServiceRolePolicy](#)
- [DynamoDBCloudWatchContributorInsightsServiceRolePolicy](#)
- [DynamoDBKinesisReplicationServiceRolePolicy](#)
- [DynamoDBReplicationServiceRolePolicy](#)
- [EC2FastLaunchFullAccess](#)
- [EC2FastLaunchServiceRolePolicy](#)
- [EC2FleetTimeShiftableServiceRolePolicy](#)
- [Ec2ImageBuilderCrossAccountDistributionAccess](#)
- [EC2ImageBuilderLifecycleExecutionPolicy](#)
- [EC2InstanceConnect](#)
- [Ec2InstanceConnectEndpoint](#)
- [EC2InstanceProfileForImageBuilder](#)
- [EC2InstanceProfileForImageBuilderECRContainerBuilds](#)
- [ECRReplicationServiceRolePolicy](#)
- [ElastiCacheServiceRolePolicy](#)
- [ElasticLoadBalancingFullAccess](#)
- [ElasticLoadBalancingReadOnly](#)
- [ElementalActivationsDownloadSoftwareAccess](#)
- [ElementalActivationsFullAccess](#)

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

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

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

- [VMImportExportRoleForAWSConnector](#)
- [VPC_Lattice_Full_Access](#)
- [VPC_Lattice_Read_Only_Access](#)
- [VPC_Lattice_Services_Invoke_Access](#)
- [WAF_Logging_Service_Role_Policy](#)
- [WAF_Regional_Logging_Service_Role_Policy](#)
- [WAF_V2_Logging_Service_Role_Policy](#)
- [Well_Architected_Console_Full_Access](#)
- [Well_Architected_Console_Read_Only_Access](#)
- [Work_Link_Service_Role_Policy](#)

AccessAnalyzerServiceRolePolicy

説明： Access Analyzer がリソースメタデータを分析できるようにする

AccessAnalyzerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 2 日 17:13 UTC
- 編集日時: 2024 年 5 月 30 日 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```

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

```
    "s3:GetMultiRegionAccessPointPolicyStatus",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets",
    "s3:ListMultiRegionAccessPoints",
    "s3express:GetBucketPolicy",
    "s3express:ListAllMyDirectoryBuckets",
    "sns:GetTopicAttributes",
    "sns:ListTopics",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetResourcePolicy",
    "secretsmanager:ListSecrets",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AdministratorAccess

説明：AWS サービスとリソースへのフルアクセスを提供します。

AdministratorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AdministratorAccess-Amplify

説明： Amplify アプリケーションに必要なリソースへの直接アクセスを明示的に許可しながら、アカウントの管理者権限を付与します。

AdministratorAccess-Amplify は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AdministratorAccess-Amplify をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 19:03 UTC
- 編集日時: 2024 年 4 月 4 日 20:35 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-Amplify

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/amplify-*"
  ]
},
{
  "Sid" : "CLIManageviaCFNPolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoleTags",
    "iam:TagRole",
    "iam:AttachRolePolicy",
    "iam:CreatePolicy",
    "iam>DeletePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePolicy",
    "iam:UntagRole",
    "iam:UpdateRole",
    "iam:GetRole",
    "iam:GetPolicy",
    "iam:GetRolePolicy",
    "iam:PassRole",
    "iam:ListPolicyVersions",
    "iam:CreatePolicyVersion",
    "iam>DeletePolicyVersion",
    "iam:CreateRole",
    "iam:ListRolePolicies",
    "iam:PutRolePermissionsBoundary",
    "iam>DeleteRolePermissionsBoundary",
    "appsync:CreateApiKey",
    "appsync:CreateDataSource",
    "appsync:CreateFunction",
    "appsync:CreateResolver",
    "appsync:CreateType",
    "appsync>DeleteApiKey",
    "appsync>DeleteDataSource",
    "appsync>DeleteFunction",
    "appsync>DeleteResolver",
    "appsync>DeleteType",
    "appsync:GetDataSource",
```

```
"appsync:GetFunction",
"appsync:GetIntrospectionSchema",
"appsync:GetResolver",
"appsync:GetSchemaCreationStatus",
"appsync:GetType",
"appsync:GraphQL",
"appsync:ListApiKeys",
"appsync:ListDataSources",
"appsync:ListFunctions",
"appsync:ListGraphQLApis",
"appsync:ListResolvers",
"appsync:ListResolversByFunction",
"appsync:ListTypes",
"appsync:StartSchemaCreation",
"appsync:UntagResource",
"appsync:UpdateApiKey",
"appsync:UpdateDataSource",
"appsync:UpdateFunction",
"appsync:UpdateResolver",
"appsync:UpdateType",
"appsync:TagResource",
"appsync:CreateGraphQLApi",
"appsync>DeleteGraphQLApi",
"appsync:GetGraphQLApi",
"appsync:ListTagsForResource",
"appsync:UpdateGraphQLApi",
"apigateway:DELETE",
"apigateway:GET",
"apigateway:PATCH",
"apigateway:POST",
"apigateway:PUT",
"cognito-idp:CreateUserPool",
"cognito-identity:CreateIdentityPool",
"cognito-identity>DeleteIdentityPool",
"cognito-identity:DescribeIdentity",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:SetIdentityPoolRoles",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:UpdateIdentityPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp>DeleteUserPool",
"cognito-idp>DeleteUserPoolClient",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
```



```
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:UpdateUserPoolClient",
"cognito-idp:CreateGroup",
"cognito-idp>DeleteGroup",
"cognito-identity:TagResource",
"cognito-idp:TagResource",
"cognito-idp:UpdateUserPool",
"cognito-idp:SetUserPoolMfaConfig",
"lambda:AddPermission",
"lambda:CreateFunction",
"lambda>DeleteFunction",
"lambda:GetFunction",
"lambda:GetFunctionConfiguration",
"lambda:InvokeAsync",
"lambda:InvokeFunction",
"lambda:RemovePermission",
"lambda:UpdateFunctionCode",
"lambda:UpdateFunctionConfiguration",
"lambda:ListTags",
"lambda:TagResource",
"lambda:UntagResource",
"lambda:AddLayerVersionPermission",
"lambda:CreateEventSourceMapping",
"lambda>DeleteEventSourceMapping",
"lambda>DeleteLayerVersion",
"lambda:GetEventSourceMapping",
"lambda:GetLayerVersion",
"lambda:ListEventSourceMappings",
"lambda:ListLayerVersions",
"lambda:PublishLayerVersion",
"lambda:RemoveLayerVersionPermission",
"lambda:UpdateEventSourceMapping",
"dynamodb:CreateTable",
"dynamodb>DeleteItem",
"dynamodb>DeleteTable",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListStreams",
"dynamodb:PutItem",
"dynamodb:TagResource",
"dynamodb:ListTagsOfResource",
"dynamodb:UntagResource",
```

```
"dynamodb:UpdateContinuousBackups",
"dynamodb:UpdateItem",
"dynamodb:UpdateTable",
"dynamodb:UpdateTimeToLive",
"s3:CreateBucket",
"s3:ListBucket",
"s3:PutBucketAcl",
"s3:PutBucketCORS",
"s3:PutBucketNotification",
"s3:PutBucketPolicy",
"s3:PutBucketWebsite",
"s3:PutObjectAcl",
"cloudfront:CreateCloudFrontOriginAccessIdentity",
"cloudfront:CreateDistribution",
"cloudfront>DeleteCloudFrontOriginAccessIdentity",
"cloudfront>DeleteDistribution",
"cloudfront:GetCloudFrontOriginAccessIdentity",
"cloudfront:GetCloudFrontOriginAccessIdentityConfig",
"cloudfront:GetDistribution",
"cloudfront:GetDistributionConfig",
"cloudfront:TagResource",
"cloudfront:UntagResource",
"cloudfront:UpdateCloudFrontOriginAccessIdentity",
"cloudfront:UpdateDistribution",
"events:DeleteRule",
"events:DescribeRule",
"events:ListRuleNamesByTarget",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"mobiletargeting:GetApp",
"kinesis:AddTagsToStream",
"kinesis:CreateStream",
"kinesis>DeleteStream",
"kinesis:DescribeStream",
"kinesis:DescribeStreamSummary",
"kinesis:ListTagsForStream",
"kinesis:PutRecords",
"es:AddTags",
"es:CreateElasticsearchDomain",
"es>DeleteElasticsearchDomain",
"es:DescribeElasticsearchDomain",
"es:UpdateElasticsearchDomainConfig",
"s3:PutEncryptionConfiguration",
```

```
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "CLISDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "appsync:GetIntrospectionSchema",
    "appsync:GraphQL",
    "appsync:UpdateApiKey",
    "appsync:ListApiKeys",
    "amplify:*",
    "amplifybackend:*",
    "amplifyuibuilder:*",
    "sts:AssumeRole",
    "mobiletargeting:*",
    "cognito-idp:AdminAddUserToGroup",
    "cognito-idp:AdminCreateUser",
    "cognito-idp:CreateGroup",
    "cognito-idp>DeleteGroup",
    "cognito-idp>DeleteUser",
    "cognito-idp:ListUsers",
    "cognito-idp:AdminGetUser",
    "cognito-idp:ListUsersInGroup",
    "cognito-idp:AdminDisableUser",
    "cognito-idp:AdminRemoveUserFromGroup",
    "cognito-idp:AdminResetUserPassword",
    "cognito-idp:AdminListGroupsForUser",
    "cognito-idp:ListGroups",
    "cognito-idp:AdminListUserAuthEvents",
    "cognito-idp:AdminDeleteUser",
    "cognito-idp:AdminConfirmSignUp",
    "cognito-idp:AdminEnableUser",
    "cognito-idp:AdminUpdateUserAttributes",
    "cognito-idp:DescribeIdentityProvider",
    "cognito-idp:DescribeUserPool",
```

```
"cognito-idp:DeleteUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:CreateUserPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp:UpdateUserPool",
"cognito-idp:AdminSetUserPassword",
"cognito-idp:ListUserPools",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListIdentityProviders",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:SetIdentityPoolRoles",
"cognito-identity:CreateIdentityPool",
"cognito-identity>DeleteIdentityPool",
"cognito-identity:ListIdentityPools",
"cognito-identity:DescribeIdentityPool",
"dynamodb:DescribeTable",
"dynamodb:ListTables",
"lambda:GetFunction",
"lambda:CreateFunction",
"lambda:AddPermission",
"lambda>DeleteFunction",
"lambda>DeleteLayerVersion",
"lambda:InvokeFunction",
"lambda:ListLayerVersions",
"iam:PutRolePolicy",
"iam:CreatePolicy",
"iam:AttachRolePolicy",
"iam:ListPolicyVersions",
"iam:ListAttachedRolePolicies",
"iam:CreateRole",
"iam:PassRole",
"iam:ListRolePolicies",
"iam>DeleteRolePolicy",
"iam:CreatePolicyVersion",
"iam>DeletePolicyVersion",
"iam>DeleteRole",
"iam:DetachRolePolicy",
"cloudformation:ListStacks",
"cloudformation:DescribeStacks",
"sns:CreateSMSSandboxPhoneNumber",
"sns:GetSMSSandboxAccountStatus",
"sns:VerifySMSSandboxPhoneNumber",
"sns>DeleteSMSSandboxPhoneNumber",
```

```
    "sns:ListSMSSandboxPhoneNumbers",
    "sns:ListOriginationNumbers",
    "rekognition:DescribeCollection",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "lex:GetBot",
    "lex:GetBuiltinIntent",
    "lex:GetBuiltinIntents",
    "lex:GetBuiltinSlotTypes",
    "cloudformation:GetTemplateSummary",
    "codecommit:GitPull",
    "cloudfront:GetCloudFrontOriginAccessIdentity",
    "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
    "polly:DescribeVoices"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifySSMCalls",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm>DeleteParameter",
    "ssm:GetParametersByPath",
    "ssm:GetParameters",
    "ssm:GetParameter",
    "ssm>DeleteParameters"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
},
{
  "Sid" : "GeoPowerUser",
  "Effect" : "Allow",
  "Action" : [
    "geo:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmplifyEcrSDKCalls",
  "Effect" : "Allow",
  "Action" : [
    "ecr:DescribeRepositories"
  ],
  "Resource" : "*"
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AdministratorAccess-AWSElasticBeanstalk

説明: アカウント管理アクセス許可を付与します。デベロッパーと管理者が AWS Elastic Beanstalk アプリケーションの管理に必要なリソースに直接アクセスすることを明示的に許可する

AdministratorAccess-AWSElasticBeanstalk は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AdministratorAccess-AWSElasticBeanstalk をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 22 日 19:36 UTC
- 編集日時: 2023 年 3 月 23 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessDeviceSetup

説明： AlexaForBusiness サービスへのデバイスセットアップアクセスを提供する

AlexaForBusinessDeviceSetup は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessDeviceSetup をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2019 年 5 月 20 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessFullAccess

説明: AlexaForBusiness リソースへのフルアクセスと、関連する へのアクセスを許可します AWS のサービス

AlexaForBusinessFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC

- 編集日時: 2020 年 7 月 1 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessGatewayExecution

説明： サービスへのゲートウェイ実行アクセス AlexaForBusiness を提供する

AlexaForBusinessGatewayExecution は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AlexaForBusinessGatewayExecution` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2017 年 11 月 30 日 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

説明： AVS デバイスへのアクセスを提供する

AlexaForBusinessLifesizeDelegatedAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessLifesizeDelegatedAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 4 日 19:46 UTC

- 編集日時: 2020 年 6 月 12 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/
AlexaForBusinessLifesizeDelegatedAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b>DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGW4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IW07UEGW4TL"
          ]
        }
      }
    }
  ]
}
```



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessNetworkProfileServicePolicy

説明：このポリシーにより、Alexa for Business はネットワークプロファイルによってスケジュールされた自動タスクを実行できます。

AlexaForBusinessNetworkProfileServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 13 日 00:53 UTC
- 編集日時: 2019 年 4 月 5 日 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessPolyDelegatedAccessPolicy

説明 : Poly AVS デバイスへのアクセスを提供する

AlexaForBusinessPolyDelegatedAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessPolyDelegatedAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 16 日 19:48 UTC
- 編集日時: 2019 年 10 月 16 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AlexaForBusinessReadOnlyAccess

説明： AlexaForBusiness サービスへの読み取り専用アクセスを提供する

AlexaForBusinessReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AlexaForBusinessReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:47 UTC
- 編集日時: 2019 年 11 月 20 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonAPIGatewayAdministrator

説明： 経由で Amazon APIs Gateway で API を作成/編集/削除するためのフルアクセスを提供します
AWS Management Console。 Amazon API Gateway

AmazonAPIGatewayAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:34 UTC
- 編集日時: 2015 年 7 月 9 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonAPIGatewayInvokeFullAccess

説明： Amazon API Gateway で APIs を呼び出すためのフルアクセスを提供します。

AmazonAPIGatewayInvokeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayInvokeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:36 UTC

- 編集日時: 2018 年 12 月 18 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonAPIGatewayPushToCloudWatchLogs

説明 : API Gateway がユーザーのアカウントにログをプッシュできるようにします。

AmazonAPIGatewayPushToCloudWatchLogs は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAPIGatewayPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 23:41 UTC
- 編集日時: 2015 年 11 月 11 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAppFlowFullAccess

説明： Amazon へのフルアクセス AppFlow と、フローのソースまたは送信先としてサポートされている AWS のサービス (S3 および Redshift) へのアクセスを提供します。また、KMS にアクセスして暗号化することもできます。

AmazonAppFlowFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppFlowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 2 日 23:30 UTC
- 編集日時: 2022 年 2 月 28 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonAppFlowReadOnlyAccess

説明： Amazon Appflow フローへの読み取り専用アクセスを提供します

AmazonAppFlowReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppFlowReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 2 日 23:26 UTC
- 編集日時: 2022 年 2 月 28 日 20:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAppStreamFullAccess

説明 : AppStream 経由で Amazon へのフルアクセスを提供します AWS Management Console。

AmazonAppStreamFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 8 月 28 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAppStreamPCAAccess

説明: 証明書ベースの認証のための顧客アカウントの AWS Certificate Manager Private CA への Amazon AppStream 2.0 アクセス

AmazonAppStreamPCAAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamPCAAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 24 日 17:05 UTC
- 編集日時: 2022 年 10 月 24 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAppStreamReadOnlyAccess

説明： AppStream 経由で Amazon への読み取り専用アクセスを提供します AWS Management Console。

AmazonAppStreamReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 12 月 7 日 21:00 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonAppStreamServiceAccess

説明: Amazon AppStream サービスロールのデフォルトポリシー。

AmazonAppStreamServiceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAppStreamServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 19 日 04:17 UTC
- 編集日時: 2020 年 6 月 26 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAthenaFullAccess

説明: Amazon Athena へのフルアクセスと、クエリ、結果の書き込み、データ管理を有効にするために必要な依存関係へのスコープ付きアクセスを提供します。

AmazonAthenaFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAthenaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 16:46 UTC
- 編集日時: 2024 年 1 月 3 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAugmentedAIFullAccess

説明 : FlowDefinitions、 、 など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセス HumanTaskUis を提供します HumanLoops。パブリッククラウドのワークチーム FlowDefinitions に対して を作成するためのアクセスを許可しません。

AmazonAugmentedAIFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:21 UTC
- 編集日時: 2019 年 12 月 3 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAugmentedAIHumanLoopFullAccess

説明： すべてのオペレーションを実行するためのアクセスを提供します HumanLoops。

AmazonAugmentedAIHumanLoopFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIHumanLoopFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:20 UTC
- 編集日時: 2019 年 12 月 3 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonAugmentedAIIntegratedAPIAccess

説明 : FlowDefinitions、 、 など、Amazon Augmented AI リソースのすべてのオペレーションを実行するためのアクセス HumanTaskUis を提供します HumanLoops。また、Amazon Augmented AI と統合されたサービスの運用にもアクセスできます。

AmazonAugmentedAIIntegratedAPIAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonAugmentedAIIntegratedAPIAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 22 日 20:47 UTC
- 編集日時: 2020 年 4 月 22 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonBedrockFullAccess

説明： Amazon Bedrock へのフルアクセスと、Amazon Bedrock が必要とする関連サービスへの制限付きアクセスを提供します。

AmazonBedrockFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 6 日 15:47 UTC
- 編集日時: 2023 年 12 月 6 日 15:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonBedrockReadOnly

説明： Amazon Bedrock への読み取り専用アクセスを提供します

AmazonBedrockReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBedrockReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 6 日 15:48 UTC
- 編集日時: 2023 年 12 月 6 日 15:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonBraketFullAccess

説明： AWS Management Console および SDK 経由で Amazon Braket へのフルアクセスを提供します。関連サービス (S3、ログなど) へのアクセスも提供します。

AmazonBraketFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBraketFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 6 日 20:12 UTC
- 編集日時: 2023 年 4 月 19 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonBraketJobsExecutionPolicy

説明: S3 AWS のサービス、Cloudwatch、IAM、Braket などの Amazon Braket ジョブの実行に必要な および リソースへのアクセスを許可します

AmazonBraketJobsExecutionPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonBraketJobsExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 26 日 19:34 UTC
- 編集日時: 2021 年 11 月 28 日 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonBraketServiceRolePolicy

説明： Amazon Braket がユーザーに代わって AWS リソースを作成および管理することを許可する

AmazonBraketServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 4 日 17:12 UTC
- 編集日時: 2020 年 8 月 6 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeFullAccess

説明： 経由で Amazon Chime 管理コンソールへのフルアクセスを提供します AWS Management Console。

AmazonChimeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:15 UTC
- 編集日時: 2020 年 12 月 14 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeReadOnly

説明： 経由で Amazon Chime 管理コンソールへの読み取り専用アクセスを提供します AWS Management Console。

AmazonChimeReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:04 UTC
- 編集日時: 2020 年 12 月 14 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeReadOnly

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeSDK

説明： Amazon Chime SDK オペレーションへのアクセスを提供します

AmazonChimeSDK は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeSDK をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 2 月 4 日 21:53 UTC
- 編集日時: 2023 年 1 月 10 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

説明： Amazon Chime SDK MediaPipelines サービスにリンクされたロールの マネージドポリシー

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 4 日 22:02 UTC
- 編集日時: 2023 年 12 月 8 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeSDKMessagingServiceRolePolicy

説明： Amazon Chime SDK メッセージングが AWS リソースにアクセスし、メッセージング機能を有効にすることを許可する

AmazonChimeSDKMessagingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 3 日 01:43 UTC
- 編集日時: 2023 年 3 月 3 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeServiceRolePolicy

説明： Amazon Chime が使用または管理する AWS リソースへのアクセスを有効にする

AmazonChimeServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:25 UTC
- 編集日時: 2019 年 9 月 30 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

説明： Amazon Chime がユーザーに代わって Amazon Transcribe と Amazon Transcribe Medical にアクセスすることを許可する

AmazonChimeTranscriptionServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 4 日 21:47 UTC

- 編集日時: 2021 年 8 月 4 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeUserManagement

説明： 経由で Amazon Chime 管理コンソールへのユーザー管理アクセスを提供します AWS Management Console。

AmazonChimeUserManagement は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonChimeUserManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 1 日 22:17 UTC
- 編集日時: 2020 年 2 月 18 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```

```
    "chime:ListDomains",
    "chime:GetDomain",
    "chime:ListDirectories",
    "chime:ListGroups",
    "chime:SubmitSupportRequest",
    "chime:ListDelegates",
    "chime:ListAccountUsageReportData",
    "chime:GetMeetingDetail",
    "chime:ListMeetingEvents",
    "chime:ListMeetingsReportData",
    "chime:GetUserActivityReportData",
    "chime:UpdateUser",
    "chime:BatchUpdateUser",
    "chime:BatchSuspendUser",
    "chime:BatchUnsuspendUser",
    "chime:AssociatePhoneNumberWithUser",
    "chime:DisassociatePhoneNumberFromUser",
    "chime:GetPhoneNumber",
    "chime:ListPhoneNumbers",
    "chime:GetUserSettings",
    "chime:UpdateUserSettings",
    "chime:CreateUser",
    "chime:AssociateSigninDelegateGroupsWithAccount",
    "chime:DisassociateSigninDelegateGroupsFromAccount"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

説明 : Amazon Chime のサービスにリンクされたロールの管理ポリシー VoiceConnector

AmazonChimeVoiceConnectorServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 9 月 30 日 22:16 UTC
- 編集日時: 2023 年 4 月 14 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudDirectoryFullAccess

説明： Amazon Cloud Directory Service へのフルアクセスを提供します。

AmazonCloudDirectoryFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudDirectoryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 25 日 00:41 UTC
- 編集日時: 2017 年 2 月 25 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudDirectoryReadOnlyAccess

説明 : Amazon Cloud Directory Service への読み取り専用アクセスを提供します。

AmazonCloudDirectoryReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudDirectoryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 28 日 23:42 UTC
- 編集日時: 2017 年 2 月 28 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchEvidentlyFullAccess

説明： Amazon CloudWatch Evidently へのフルアクセスのみを提供します。また、関連する Amazon S3、Amazon SNS、Amazon CloudWatch、およびその他の関連サービスへのアクセスも提供します。

AmazonCloudWatchEvidentlyFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchEvidentlyFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:10 UTC
- 編集日時: 2021 年 11 月 29 日 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

説明： Amazon CloudWatch Evidently への読み取り専用アクセスを提供します

AmazonCloudWatchEvidentlyReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchEvidentlyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 11 月 29 日 15:08 UTC
- 編集日時: 2021 年 11 月 29 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

説明 : CloudWatch Evidently Service が顧客に代わって関連する AWS リソースを管理できるようにします

AmazonCloudWatchEvidentlyServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 13 日 17:25 UTC
- 編集日時: 2022 年 9 月 13 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchRUMFullAccess

説明 : Amazon CloudWatch RUM サービスへのフルアクセス許可を付与します

AmazonCloudWatchRUMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchRUMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 15:46 UTC
- 編集日時: 2021 年 11 月 29 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchRUMReadOnlyAccess

説明： Amazon CloudWatch RUM サービスの読み取り専用アクセス許可を付与します

AmazonCloudWatchRUMReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCloudWatchRUMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 11 月 29 日 15:43 UTC
- 編集日時: 2022 年 10 月 28 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCloudWatchRUMServiceRolePolicy

説明： Amazon CloudWatch RUM Service に、モニタリングデータを他の関連 AWS サービスに発行するアクセス許可を付与します

AmazonCloudWatchRUMServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 23:17 UTC
- 編集日時: 2023 年 2 月 22 日 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeCatalystFullAccess

説明： Amazon へのフルアクセスを提供します CodeCatalyst

AmazonCodeCatalystFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeCatalystFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 4 月 20 日 16:50 UTC
- 編集日時: 2023 年 4 月 20 日 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeCatalystReadOnlyAccess

説明： Amazon への読み取り専用アクセスを提供します CodeCatalyst

AmazonCodeCatalystReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeCatalystReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 20 日 16:49 UTC
- 編集日時: 2023 年 4 月 20 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeCatalystSupportAccess

説明： Amazon CodeCatalyst がユーザーに代わって AWS Support ケースを作成、更新、解決できるようにします。

AmazonCodeCatalystSupportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeCatalystSupportAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 12:34 UTC

- 編集日時: 2023 年 4 月 20 日 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruProfilerAgentAccess

説明： Amazon CodeGuru Profiler エージェントに必要なアクセスを提供します。

AmazonCodeGuruProfilerAgentAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerAgentAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 5 日 22:11 UTC
- 編集日時: 2022 年 5 月 5 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruProfilerFullAccess

説明 : Amazon CodeGuru Profiler へのフルアクセスを提供します。

AmazonCodeGuruProfilerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 10:13 UTC
- 編集日時: 2020 年 7 月 15 日 03:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruProfilerReadOnlyAccess

説明： Amazon CodeGuru Profiler への読み取り専用アクセスを提供します。

AmazonCodeGuruProfilerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruProfilerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 10:30 UTC
- 編集日時: 2020 年 6 月 27 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruReviewerFullAccess

説明： Amazon CodeGuru Reviewer へのフルアクセスと、必要な依存関係へのスコープ付きアクセスを許可します。

AmazonCodeGuruReviewerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruReviewerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 8 月 29 日 04:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruReviewerReadOnlyAccess

説明 : Amazon CodeGuru Reviewer への読み取り専用アクセスを提供します。

AmazonCodeGuruReviewerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruReviewerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 08:48 UTC
- 編集日時: 2020 年 8 月 29 日 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruReviewerServiceRolePolicy

説明： Amazon CodeGuru Reviewer がユーザーに代わって リソースにアクセスするために必要なサービスにリンクされたロール。

AmazonCodeGuruReviewerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 05:31 UTC
- 編集日時: 2020 年 11 月 27 日 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

ポリシーのバージョニング

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruSecurityFullAccess

説明： Amazon CodeGuru Security へのフルアクセスを提供します。

AmazonCodeGuruSecurityFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 9 日 21:03 UTC
- 編集日時: 2023 年 5 月 9 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCodeGuruSecurityScanAccess

説明： Amazon CodeGuru Security スキャンの操作に必要なアクセスを提供します。

AmazonCodeGuruSecurityScanAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCodeGuruSecurityScanAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 9 日 20:54 UTC
- 編集日時: 2023 年 5 月 9 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoDeveloperAuthenticatedIdentities

説明: 認証バックエンドからデベロッパーが認証した ID をサポートする Amazon Cognito APIs へのアクセスを提供します。

AmazonCognitoDeveloperAuthenticatedIdentities は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonCognitoDeveloperAuthenticatedIdentities` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:22 UTC
- 編集日時: 2015 年 3 月 24 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoIdpEmailServiceRolePolicy

説明 : Amazon Cognito ユーザープールサービスが E メール送信に SES ID を使用することを許可する

AmazonCognitoIdpEmailServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 3 月 21 日 21:32 UTC
- 編集日時: 2019 年 3 月 21 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoIdpServiceRolePolicy

説明 : Amazon Cognito ユーザープールが使用または管理する AWS のサービス およびリソースへのアクセスを有効にする

AmazonCognitoIdpServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:30 UTC
- 編集日時: 2020 年 6 月 26 日 22:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoPowerUser

説明：既存の Amazon Cognito リソースへの管理アクセスを提供します。新しい Cognito リソースを作成するには、AWS アカウント 管理者権限が必要です。

AmazonCognitoPowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:14 UTC
- 編集日時: 2021 年 6 月 1 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoReadOnly

説明： Amazon Cognito リソースへの読み取り専用アクセスを提供します。

AmazonCognitoReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 3 月 24 日 17:06 UTC
- 編集日時: 2019 年 8 月 1 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

説明：このポリシーは、Cognito ID プールの認証されていない ID に許可される一連のアクセス許可を定義します。このポリシーは、スタンドアロンのアクセス許可ポリシーとして使用することを意図したものではありません。アイデンティティプール内のロールにアタッチされている過度に許容度の高いポリシーに対するガードレールとして使用されます。このポリシーはどのロールにもアタッチしないでください。Cognito Identity Service は、認証情報を作成するときに、このポリシーをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティティに関連付

けられたロールと、Cognito が所有するこの管理ポリシーで付与される権限の共通部分によって定義されるようになりました。

AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 19 日 23:04 UTC
- 編集日時: 2023 年 7 月 19 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthenticatedIdentitiesSessionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonCognitoUnauthenticatedIdentities

説明：このポリシーは、Cognito ID プールの認証されていない ID に許可される一連のアクセス許可を定義します。これを unauth ロールにアタッチする必要はありません。Cognito Identity Service は、認証情報を作成するときに、このロールをスコープダウンポリシーとして自動的に含めます。拡張フローを通じて他の AWS リソースに一時的にアクセスする権限は、サービスによって提供される認証されていないユーザーのアイデンティティに関連付けられたロールと、Cognito が所有するこの管理ポリシーで付与される権限の共通部分によって定義されるようになりました。

AmazonCognitoUnauthenticatedIdentities は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonCognitoUnauthenticatedIdentities をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 1 日 22:36 UTC
- 編集日時: 2023 年 2 月 1 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonConnect_FullAccess

説明: このポリシーの目的は、AWS Connect リソースの使用に必要なアクセス許可を Connect ユーザーに付与することです。このポリシーは、AWS Connect コンソールとパブリック APIs

AmazonConnect_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnect_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 20 日 19:54 UTC
- 編集日時: 2023 年 3 月 7 日 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]
}

```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

説明： Amazon Connect Campaigns サービスリンクロールのポリシー

AmazonConnectCampaignsServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 23 日 20:54 UTC
- 編集日時: 2023 年 11 月 8 日 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonConnectReadOnlyAccess

説明: 内の Amazon Connect インスタンスを表示するアクセス許可を付与します AWS アカウント。

AmazonConnectReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 10 月 17 日 21:00 UTC
- 編集日時: 2019 年 11 月 6 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonConnectServiceLinkedRolePolicy

説明： Amazon Connect がユーザーに代わって AWS リソースを作成および管理できるようにします。

AmazonConnectServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 9 月 7 日 00:21 UTC
- 編集日時: 2024 年 5 月 24 日 01:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v16 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

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



```
    "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
  ]
},
{
  "Sid" : "AllowListIntegrationForCustomerProfile",
  "Effect" : "Allow",
  "Action" : [
    "profile:ListAccountIntegrations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowReadForCustomerProfileObjectTemplates",
  "Effect" : "Allow",
  "Action" : [
    "profile:ListProfileObjectTypeTemplates",
    "profile:GetProfileObjectTypeTemplate"
  ],
  "Resource" : "arn:aws:profile:*:*:/templates*"
},
{
  "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
  "Effect" : "Allow",
  "Action" : [
    "wisdom:CreateContent",
    "wisdom:DeleteContent",
    "wisdom:CreateKnowledgeBase",
    "wisdom:GetAssistant",
    "wisdom:GetKnowledgeBase",
    "wisdom:GetContent",
    "wisdom:GetRecommendations",
    "wisdom:GetSession",
    "wisdom:NotifyRecommendationsReceived",
    "wisdom:QueryAssistant",
    "wisdom:StartContentUpload",
    "wisdom:UpdateContent",
    "wisdom:UntagResource",
    "wisdom:TagResource",
    "wisdom:CreateSession",
    "wisdom:CreateQuickResponse",
    "wisdom:GetQuickResponse",
    "wisdom:SearchQuickResponses",
    "wisdom:StartImportJob",
    "wisdom:GetImportJob",
```

```
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom>DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
    }
},
{
    "Sid" : "AllowListOperationForWisdom",
    "Effect" : "Allow",
    "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
    "Effect" : "Allow",
    "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile>CreateCalculatedAttributeDefinition",
        "profile>DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
    ],
    "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
    ]
},
{
    "Sid" : "AllowPutMetricsForConnectNamespace",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
```

```
        "cloudwatch:namespace" : "AWS/Connect"
    }
}
},
{
    "Sid" : "AllowSMSVoiceOperationsForConnect",
    "Effect" : "Allow",
    "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
    ],
    "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
    "Effect" : "Allow",
    "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
    ],
    "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
    }
},
{
    "Sid" : "AllowWritePermissionForCustomerProfileObjects",
    "Effect" : "Allow",
    "Action" : [
        "profile:PutProfileObject"
    ],
    "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
    ]
}
]
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonConnectSynchronizationServiceRolePolicy

説明： Amazon Connect がユーザーに代わってリージョン間で AWS リソースを同期できるようにします。

AmazonConnectSynchronizationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 27 日 22:38 UTC
- 編集日時: 2023 年 10 月 27 日 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonConnectVoiceIDFullAccess

説明： Amazon Connect Voice ID へのフルアクセスを提供します

AmazonConnectVoiceIDFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonConnectVoiceIDFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 26 日 19:04 UTC
- 編集日時: 2021 年 9 月 26 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneDomainExecutionRolePolicy

説明： Amazon DataZone DomainExecutionRole のサービスロールのデフォルトポリシー。このロールは、Amazon DataZone ドメイン内のデータをカタログ化、検出、管理、共有、分析 DataZone するために Amazon によって使用されます。

AmazonDataZoneDomainExecutionRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneDomainExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 27 日 21:55 UTC
- 編集日時: 2024 年 4 月 1 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

説明: Amazon DataZone は、データ分析アクションを実行するための環境用の IAM ロールを作成し、これらのロールを作成するときにこのポリシーを使用してアクセス許可の境界を定義します。

AmazonDataZoneEnvironmentRolePermissionsBoundary は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneEnvironmentRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 11 日 23:38 UTC
- 編集日時: 2023 年 11 月 17 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Sid" : "CreateGlueConnection",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Resource" : [
  "arn:aws:ec2:*:*:network-interface/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "aws-glue-service-resource"
    ]
  }
}
},
{
  "Sid" : "GlueOperations",
  "Effect" : "Allow",
  "Action" : [
    "glue:*DataQuality*",
    "glue:BatchCreatePartition",
    "glue:BatchDeleteConnection",
    "glue:BatchDeletePartition",
    "glue:BatchDeleteTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:BatchStopJobRun",
    "glue:BatchUpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "glue:CreateDatabase",
    "glue:CreateJob",
    "glue:CreatePartition",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:CreateWorkflow",
    "glue>DeleteBlueprint",
    "glue>DeleteColumnStatisticsForPartition",
    "glue>DeleteColumnStatisticsForTable",
    "glue>DeleteConnection",
```

```
"glue:DeleteCrawler",
"glue:DeleteJob",
"glue:DeletePartition",
"glue:DeletePartitionIndex",
"glue:DeleteTable",
"glue:DeleteTableVersion",
"glue:DeleteWorkflow",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:PutWorkflowRunProperties",
"glue:ResetJobBookmark",
"glue:ResumeWorkflowRun",
"glue:SearchTables",
"glue:StartBlueprintRun",
"glue:StartCrawler",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:StopCrawler",
"glue:StopCrawlerSchedule",
"glue:StopWorkflowRun",
"glue:UpdateBlueprint",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateConnection",
"glue:UpdateCrawler",
"glue:UpdateCrawlerSchedule",
"glue:UpdateDatabase",
"glue:UpdateJob",
"glue:UpdatePartition",
"glue:UpdateTable",
"glue:UpdateWorkflow"
],
"Resource" : "*",
```

```
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
      }
    }
  },
  {
    "Sid" : "PassRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/datazone*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "glue.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SameAccountKmsOperations",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:Decrypt",
      "kms:ListKeys"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringNotEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "KmsOperationsWithResourceTag",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:Decrypt",
      "kms:ListKeys",
      "kms:Encrypt",
```

```
    "kms:GenerateDataKey",
    "kms:Verify",
    "kms:Sign"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AnalyticsOperations",
  "Effect" : "Allow",
  "Action" : [
    "datazone:*",
    "sqlworkbench:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QueryOperations",
  "Effect" : "Allow",
  "Action" : [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena>DeleteNamedQuery",
    "athena>DeleteNotebook",
    "athena>DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
```



```
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatements",
"athena:ListQueryExecutions",
"athena:ListTableMetadata",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"athena:StartCalculationExecution",
"athena:StartQueryExecution",
"athena:StartSession",
"athena:StopCalculationExecution",
"athena:StopQueryExecution",
"athena:TerminateSession",
"athena:UpdateNamedQuery",
"athena:UpdateNotebook",
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:Describe*",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition",
"glue:BatchDeleteTable",
"glue:BatchDeleteTableVersion",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetWorkflows",
"glue:BatchUpdatePartition",
"glue:CreateBlueprint",
"glue:CreateConnection",
"glue:CreateCrawler",
"glue:CreateDatabase",
"glue:CreateJob",
"glue:CreatePartition",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:CreateWorkflow",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue>DeletePartition",
"glue>DeletePartitionIndex",
```

```
"glue:DeleteTable",
"glue:DeleteTableVersion",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:GetConnection",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetPartition",
"glue:GetPartitions",
"glue:ListSchemas",
"glue:ListJobs",
"glue:NotifyEvent",
"glue:SearchTables",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:UpdateDatabase",
"glue:UpdatePartition",
"glue:UpdateTable",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:ListGroups",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListUsers",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:DescribeMetricFilters",
"logs:DescribeQueries",
"logs:DescribeQueryDefinitions",
"logs:DescribeMetricFilters",
"logs:StartQuery",
"logs:StopQuery",
"logs:GetLogEvents",
"logs:GetLogGroupFields",
"logs:GetQueryResults",
"logs:GetLogRecord",
"logs:PutLogEvents",
"logs:CreateLogStream",
"logs:FilterLogEvents",
"lakeformation:GetDataAccess",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetResourceLFTags",
```

```
    "lakeformation:ListPermissions",
    "redshift-data:ListTables",
    "redshift-data:DescribeTable",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:DescribeStatement",
    "redshift:CreateClusterUser",
    "redshift:DescribeClusters",
    "redshift:DescribeDataShares",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:JoinGroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "secretsmanager:ListSecrets",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "QueryOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "athena:GetQueryResultsStream"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "SecretsManagerOperationsWithTagKeys",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource"
  ]
},
```

```
"Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
"Condition" : {
  "StringLike" : {
    "aws:ResourceTag/AmazonDataZoneDomain" : "*",
    "aws:ResourceTag/AmazonDataZoneProject" : "*"
  },
  "Null" : {
    "aws:TagKeys" : "false"
  },
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "AmazonDataZoneDomain",
      "AmazonDataZoneProject"
    ]
  }
},
{
  "Sid" : "DataZoneS3Buckets",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject"
  ],
  "Resource" : [
    "arn:aws:s3::*:/datazone/*"
  ]
},
{
  "Sid" : "DataZoneS3BucketLocation",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListDataZoneS3Bucket",
```

```
"Effect" : "Allow",
"Action" : [
  "s3:ListBucket"
],
"Resource" : [
  "*"
],
"Condition" : {
  "StringLike" : {
    "s3:prefix" : [
      "*/datazone/*",
      "datazone/*"
    ]
  }
}
},
{
  "Sid" : "NotDeniedOperations",
  "Effect" : "Deny",
  "NotAction" : [
    "datzone:*",
    "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" : [
  "*"
]
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneFullAccess

説明： DataZone 経由で Amazon へのフルアクセスと AWS Management Console、Amazon が必要とする関連サービスへの制限付きアクセスを提供します。

AmazonDataZoneFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 20:06 UTC
- 編集日時: 2024 年 4 月 23 日 21:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",

```

```
    "iam:ListRoles",
    "sso:DescribeRegisteredRegions",
    "s3:ListAllMyBuckets",
    "redshift:DescribeClusters",
    "redshift-serverless:ListWorkgroups",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "BucketReadOnlyStatement",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Sid" : "CreateBucketStatement",
  "Effect" : "Allow",
  "Action" : "s3:CreateBucket",
  "Resource" : "arn:aws:s3:::amazon-datazone*"
},
{
  "Sid" : "RamCreateResourceStatement",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "ram:RequestedResourceType" : "datazone:Domain"
    }
  }
},
{
  "Sid" : "RamResourceStatement",
```

```
"Effect" : "Allow",
"Action" : [
  "ram:DeleteResourceShare",
  "ram:AssociateResourceShare",
  "ram:DisassociateResourceShare",
  "ram:RejectResourceShareInvitation"
],
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "ram:ResourceShareName" : [
      "DataZone*"
    ]
  }
}
},
{
  "Sid" : "RamResourceReadOnlyStatement",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShares",
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IAMPassRoleStatement",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : [
    "arn:aws:iam::*:role/AmazonDataZone*",
    "arn:aws:iam::*:role/service-role/AmazonDataZone*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:passedToService" : "datazone.amazonaws.com"
    }
  }
}
},
{
  "Sid" : "IAMGetPolicyStatement",
  "Effect" : "Allow",
  "Action" : "iam:GetPolicy",
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneFullUserAccess

説明: Amazon へのフルアクセスを提供しますが DataZone、ドメイン、ユーザー、または関連するアカウントの管理は許可しません。

AmazonDataZoneFullUserAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneFullUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 21:06 UTC
- 編集日時: 2024 年 4 月 1 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

ポリシーのバージョニング

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

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



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneGlueManageAccessRolePolicy

説明: このポリシーは、Amazon がデータ DataZone への発行とアクセス許可を有効にするためのアクセス許可を付与します。

AmazonDataZoneGlueManageAccessRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneGlueManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:21 UTC
- 編集日時: 2024 年 6 月 3 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
```

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

```
    }
  },
  {
    "Sid" : "LakeformationResourceSharingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:BatchGrantPermissions",
      "lakeformation:BatchRevokePermissions",
      "lakeformation:CreateLakeFormationOptIn",
      "lakeformation>DeleteLakeFormationOptIn",
      "lakeformation:GrantPermissions",
      "lakeformation:GetResourceLFTags",
      "lakeformation:ListLakeFormationOptIns",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "glue:GetDatabase",
      "glue:GetTable",
      "organizations:DescribeOrganization",
      "ram:GetResourceShareInvitations",
      "ram:ListResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CrossAccountRAMResourceSharingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "glue>DeleteResourcePolicy",
      "glue:PutResourcePolicy"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*",
      "arn:aws:glue:*:*:table/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "ram.amazonaws.com"
        ]
      }
    }
  }
},
```

```
{
  "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIfExists" : {
      "ram:RequestedResourceType" : [
        "glue:Table",
        "glue:Database",
        "glue:Catalog"
      ]
    }
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "lakeformation.amazonaws.com"
    ]
  }
},
{
  "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:AcceptResourceShareInvitation"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram>DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram>ListResourceSharePermissions",
    "ram:UpdateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
```

```
    "ram:ResourceShareName" : [
      "LakeFormation*"
    ]
  },
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "lakeformation.amazonaws.com"
    ]
  }
},
{
  "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
  "Effect" : "Allow",
  "Action" : "ram:AssociateResourceSharePermission",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "lakeformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "KMSDecryptPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/datazone:projectId" : "proj-all"
    }
  }
},
{
  "Sid" : "GetRoleForDataZone",
  "Effect" : "Allow",
  "Action" : [
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZonePortalFullAccessPolicy

説明 : DataZone APIs

AmazonDataZonePortalFullAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePortalFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 26 日 18:24 UTC
- 編集日時: 2023 年 3 月 26 日 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZonePreviewConsoleFullAccess

説明： DataZone 経由で Amazon のプレビューリリースへのフルアクセスを提供します AWS Management Console。関連サービスへの限定アクセスも提供します。

AmazonDataZonePreviewConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZonePreviewConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 28 日 15:16 UTC
- 編集日時: 2023 年 7 月 13 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

説明: Amazon DataZone は、データ分析プロジェクトのデプロイに使用する IAM ロールを作成します。は、これらのロールを作成するときにこのポリシー DataZone を使用して、アクセス許可の境界を定義します。

AmazonDataZoneProjectDeploymentPermissionsBoundary は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonDataZoneProjectDeploymentPermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 21 日 02:54 UTC
- 編集日時: 2023 年 4 月 4 日 02:48 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneProjectDeploymentPermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneProjectRolePermissionsBoundary

説明: Amazon DataZone は、データ分析アクションを実行するプロジェクトの IAM ロールを作成し、これらのロールを作成するときにこのポリシーを使用してアクセス許可の境界を定義します。

AmazonDataZoneProjectRolePermissionsBoundary は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneProjectRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 21 日 02:51 UTC
- 編集日時: 2023 年 3 月 21 日 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

説明: Amazon DataZone は、データのカタログ化、検出、管理、共有、分析を可能にするデータ管理サービスです。Amazon では DataZone、アカウントおよびサポートされているリージョン間でデータを共有してアクセスできます。Amazon は、Amazon Redshift、Amazon Athena、Glue、Lake Formation など、AWS のサービス全体のエクスペリエンス DataZone を簡素化します。AWS AWS

AmazonDataZoneRedshiftGlueProvisioningPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneRedshiftGlueProvisioningPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 22 日 20:19 UTC
- 編集日時: 2024 年 3 月 12 日 16:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

説明：このポリシーは、Amazon Redshift データをカタログに発行するアクセス DataZone 許可を Amazon に付与します。また、カタログ内の Amazon Redshift または Amazon Redshift Serverless が公開したアセットへのアクセスを許可または取り消すアクセス DataZone 許可も Amazon に付与します。

AmazonDataZoneRedshiftManageAccessRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneRedshiftManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 9 月 22 日 20:15 UTC
- 編集日時: 2023 年 11 月 16 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

説明 : AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary ポリシーは、Amazon によってプロビジョニングされた SageMaker 環境で作成された実行ロールで許可されるアクセス許可のリストです DataZone。

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:01 UTC

- 編集日時：2024 年 5 月 8 日 02:03 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ]
    }
  ]
}
```

```
    "Resource" : "arn:aws:sagemaker:*:*:*/*"
  },
  {
    "Sid" : "AllowLakeFormation",
    "Effect" : "Allow",
    "Action" : [
      "lakeformation:GetDataAccess"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAddTagsForAppAndSpace",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:AddTags"
    ],
    "Resource" : [
      "arn:aws:sagemaker:*:*:app/*",
      "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "sagemaker:TaggingAction" : [
          "CreateApp",
          "CreateSpace"
        ]
      }
    }
  },
  {
    "Sid" : "AllowStudioActions",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreatePresignedDomainUrl",
      "sagemaker:DescribeApp",
      "sagemaker:DescribeDomain",
      "sagemaker:DescribeSpace",
      "sagemaker:DescribeUserProfile",
      "sagemaker:ListApps",
      "sagemaker:ListDomains",
      "sagemaker:ListSpaces",
      "sagemaker:ListUserProfiles"
    ],
    "Resource" : "*"
  }
```

```
  },
  {
    "Sid" : "AllowAppActionsForUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  },
  {
    "Sid" : "AllowAppActionsForSharedSpaces",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition" : {
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Shared"
        ]
      }
    }
  },
  {
    "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker>DeleteSpace",
      "sagemaker:UpdateSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "Null" : {
        "sagemaker:OwnerUserProfileArn" : "true"
      }
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker>DeleteSpace",
      "sagemaker:UpdateSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private",
          "Shared"
        ]
      }
    }
  }
},
{
  "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker>CreateApp",
    "sagemaker>DeleteApp"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
  "Condition" : {
    "ArnLike" : {
      "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals" : {
      "sagemaker:SpaceSharingType" : [
        "Private"
      ]
    }
  }
},
},
```

```
{
  "Sid" : "AllowFlowDefinitionActions",
  "Effect" : "Allow",
  "Action" : "sagemaker:*",
  "Resource" : [
    "arn:aws:sagemaker:*:*:flow-definition/*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "sagemaker:WorkteamType" : [
        "private-crowd",
        "vendor-crowd"
      ]
    }
  }
},
{
  "Sid" : "AllowAWSServiceActions",
  "Effect" : "Allow",
  "Action" : [
    "sqlworkbench:*",
    "datazone:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
```

```
"codecommit:List*",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:StartImageScan",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"fsx:DescribeFileSystems",
"groundtruthlabeling:*",
"iam:GetRole",
"iam:ListRoles",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs>DeleteLogDelivery",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:UpdateLogDelivery",
"redshift-data:BatchExecuteStatement",
"redshift-data:CancelStatement",
"redshift-data:DescribeStatement",
"redshift-data:DescribeTable",
```

```
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowRAMInvitation",
  "Effect" : "Allow",
  "Action" : "ram:AcceptResourceShareInvitation",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ram:ResourceShareName" : "dzd_*"
    }
  }
},
{
  "Sid" : "AllowECRActions",
  "Effect" : "Allow",
  "Action" : [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr>DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr>DeleteRepository",
    "ecr:PutImage",
```

```
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/sagemaker*",
    "arn:aws:ecr:*:*:repository/datazone*"
  ]
},
{
  "Sid" : "AllowCodeCommitActions",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:GitPull",
    "codecommit:GitPush"
  ],
  "Resource" : [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
  ]
},
{
  "Sid" : "AllowCodeBuildActions",
  "Action" : [
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowStepFunctionsActions",
  "Action" : [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:statemachine:*sagemaker*",

```



```
    "arn:aws:states:*:*:execution:*sagemaker*:*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowSecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
  ]
},
{
  "Sid" : "AllowServiceCatalogProvisionProduct",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:ProvisionProduct"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
},
{
  "Sid" : "AllowS3ObjectActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
```

```
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl"
  ],
  "Resource" : [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
  ]
},
{
  "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*"
  ],
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/SageMaker" : "true"
    }
  }
},
{
  "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*"
  ]
},
```

```
"Condition" : {
  "StringEquals" : {
    "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
  }
},
{
  "Sid" : "AllowS3BucketActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors"
  ],
  "Resource" : [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
  ]
},
{
  "Sid" : "ReadSageMakerJumpstartArtifacts",
  "Effect" : "Allow",
  "Action" : "s3:GetObject",
  "Resource" : [
    "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
  ]
},
{
```

```
"Sid" : "AllowLambdaInvokeFunction",
"Effect" : "Allow",
"Action" : [
  "lambda:InvokeFunction"
],
"Resource" : [
  "arn:aws:lambda:*:*:function:*SageMaker*",
  "arn:aws:lambda:*:*:function:*sagemaker*",
  "arn:aws:lambda:*:*:function:*Sagemaker*",
  "arn:aws:lambda:*:*:function:*LabelingFunction*"
]
},
{
  "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowSNSActions",
  "Effect" : "Allow",
  "Action" : [
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sagemaker*"
  ]
},
{
  "Sid" : "AllowPassRoleForSageMakerRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
}
```

```
"Resource" : [
  "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
],
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "glue.amazonaws.com",
      "bedrock.amazonaws.com",
      "states.amazonaws.com",
      "lakeformation.amazonaws.com",
      "events.amazonaws.com",
      "sagemaker.amazonaws.com",
      "forecast.amazonaws.com"
    ]
  }
},
{
  "Sid" : "CrossAccountKmsOperations",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "KmsOperationsWithResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant"
  ],
  "Resource" : "*",
```

```
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
  }
},
{
  "Sid" : "AllowAthenaActions",
  "Effect" : "Allow",
  "Action" : [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena>DeleteNamedQuery",
    "athena>DeleteNotebook",
    "athena>DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
```

```

    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowGlueCreateDatabase",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
  ]
},
{
  "Sid" : "AllowRedshiftGetClusterCredentials",
  "Effect" : "Allow",
  "Action" : [
    "redshift:GetClusterCredentials"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
  "Sid" : "AllowListTags",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTags"
  ],
  "Resource" : [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
  ]
}

```

```
  },
  {
    "Sid" : "AllowCloudformationListStackResources",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:ListStackResources"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
  },
  {
    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetColumnStatisticsForPartition",
      "glue:GetColumnStatisticsForTable",
      "glue:ListJobs",
      "glue:CreateSession",
      "glue:RunStatement",
      "glue:BatchCreatePartition",
      "glue:CreatePartitionIndex",
      "glue:CreateTable",
      "glue:BatchGetWorkflows",
      "glue:BatchUpdatePartition",
      "glue:BatchDeletePartition",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:UpdateTable",
      "glue>DeleteTableVersion",
      "glue>DeleteTable",
      "glue>DeleteColumnStatisticsForPartition",
      "glue>DeleteColumnStatisticsForTable",
      "glue>DeletePartitionIndex",
      "glue:UpdateColumnStatisticsForPartition",
      "glue:UpdateColumnStatisticsForTable",
      "glue:BatchDeleteTableVersion",
      "glue:BatchDeleteTable",
      "glue:CreatePartition",
      "glue>DeletePartition",
      "glue:UpdatePartition",
      "glue:CreateBlueprint",
      "glue:CreateJob",
      "glue:CreateConnection",
      "glue:CreateCrawler",
      "glue:CreateDataQualityRuleset",
```



```
    "glue:CreateWorkflow",
    "glue:GetDatabases",
    "glue:GetTables",
    "glue:GetTable",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:ListSchemas",
    "glue:BatchGetJobs",
    "glue:GetConnection",
    "glue:GetDatabase"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowGlueActionsWithEnvironmentTag",
  "Effect" : "Allow",
  "Action" : [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue>DeleteJob",
    "glue>DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue>DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
    "glue>DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue>DeleteConnection",
```

```
    "glue:UpdateConnection",
    "glue:GetConnection",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
  }
},
{
  "Sid" : "AllowGlueDefaultAccess",
  "Effect" : "Allow",
  "Action" : [
    "glue:BatchGet*",
    "glue:Get*",
    "glue:SearchTables",
    "glue:List*",
    "glue:RunStatement"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:connection/dz-sm-*",
    "arn:aws:glue:*:*:session/*"
  ]
},
{
  "Sid" : "AllowRedshiftClusterActions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters"
  ],
  "Resource" : [
```

```
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
    ]
},
{
    "Sid" : "AllowCreateClusterUser",
    "Effect" : "Allow",
    "Action" : [
        "redshift:CreateClusterUser"
    ],
    "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
    ]
},
{
    "Sid" : "AllowCreateSecretActions",
    "Effect" : "Allow",
    "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*",
            "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
            "aws:TagKeys" : "false",
            "aws:ResourceTag/AmazonDataZoneProject" : "false",
            "aws:ResourceTag/AmazonDataZoneDomain" : "false",
            "aws:RequestTag/AmazonDataZoneDomain" : "false",
            "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneDomain",
                "AmazonDataZoneProject"
            ]
        }
    }
},
{
    "Sid" : "ForecastOperations",
```

```
"Effect" : "Allow",
"Action" : [
  "forecast:CreateExplainabilityExport",
  "forecast:CreateExplainability",
  "forecast:CreateForecastEndpoint",
  "forecast:CreateAutoPredictor",
  "forecast:CreateDatasetImportJob",
  "forecast:CreateDatasetGroup",
  "forecast:CreateDataset",
  "forecast:CreateForecast",
  "forecast:CreateForecastExportJob",
  "forecast:CreatePredictorBacktestExportJob",
  "forecast:CreatePredictor",
  "forecast:DescribeExplainabilityExport",
  "forecast:DescribeExplainability",
  "forecast:DescribeAutoPredictor",
  "forecast:DescribeForecastEndpoint",
  "forecast:DescribeDatasetImportJob",
  "forecast:DescribeDataset",
  "forecast:DescribeForecast",
  "forecast:DescribeForecastExportJob",
  "forecast:DescribePredictorBacktestExportJob",
  "forecast:GetAccuracyMetrics",
  "forecast:InvokeForecastEndpoint",
  "forecast:GetRecentForecastContext",
  "forecast:DescribePredictor",
  "forecast:TagResource",
  "forecast>DeleteResourceTree"
],
"Resource" : [
  "arn:aws:forecast:*:*:*Canvas*"
]
},
{
  "Sid" : "RDSOperation",
  "Effect" : "Allow",
  "Action" : "rds:DescribeDBInstances",
  "Resource" : "*"
},
{
  "Sid" : "AllowEventBridgeRule",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
```

```
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:PutTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeTagBasedOperations",
    "Effect" : "Allow",
    "Action" : [
      "events:TagResource"
    ],
    "Resource" : "arn:aws:events:*:*:rule/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
        "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
      }
    }
  },
  {
    "Sid" : "EventBridgeListTagOperation",
    "Effect" : "Allow",
    "Action" : "events:ListTagsForResource",
    "Resource" : "*"
  },
  {
    "Sid" : "AllowEMR",
```

```
"Effect" : "Allow",
"Action" : [
  "elasticmapreduce:DescribeCluster",
  "elasticmapreduce:ListInstanceGroups",
  "elasticmapreduce:ListClusters"
],
"Resource" : "*"
},
{
  "Sid" : "AllowSSOAction",
  "Effect" : "Allow",
  "Action" : [
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DenyNotAction",
  "Effect" : "Deny",
  "NotAction" : [
    "sagemaker:*",
    "sagemaker-geospatial:*",
    "sqlworkbench:*",
    "datazone:*",
    "forecast:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena>DeleteNamedQuery",
```

```
"athena:DeleteNotebook",
"athena:DeletePreparedStatement",
"athena:ExportNotebook",
"athena:GetDatabase",
"athena:GetDataCatalog",
"athena:GetNamedQuery",
"athena:GetPreparedStatement",
"athena:GetQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryResultsStream",
"athena:GetQueryRuntimeStatistics",
"athena:GetTableMetadata",
"athena:GetWorkGroup",
"athena:ImportNotebook",
"athena:ListDatabases",
"athena:ListDataCatalogs",
"athena:ListEngineVersions",
"athena:ListNamedQueries",
"athena:ListPreparedStatements",
"athena:ListQueryExecutions",
"athena:ListTableMetadata",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"athena:StartCalculationExecution",
"athena:StartQueryExecution",
"athena:StartSession",
"athena:StopCalculationExecution",
"athena:StopQueryExecution",
"athena:TerminateSession",
"athena:UpdateNamedQuery",
"athena:UpdateNotebook",
"athena:UpdateNotebookMetadata",
"athena:UpdatePreparedStatement",
"aws-marketplace:ViewSubscriptions",
"cloudformation:GetTemplateSummary",
"cloudformation:ListStackResources",
"cloudwatch:DeleteAlarms",
"cloudwatch:DescribeAlarms",
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cloudwatch:PutMetricAlarm",
"cloudwatch:PutMetricData",
"codebuild:BatchGetBuilds",
```

```
"codebuild:StartBuild",
"codecommit:BatchGetRepositories",
"codecommit:CreateRepository",
"codecommit:GetRepository",
"codecommit:List*",
"codecommit:GitPull",
"codecommit:GitPush",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:CreateRepository",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:SetRepositoryPolicy",
"ecr:CompleteLayerUpload",
"ecr:BatchDeleteImage",
"ecr:UploadLayerPart",
"ecr>DeleteRepositoryPolicy",
"ecr:InitiateLayerUpload",
"ecr>DeleteRepository",
"ecr:PutImage",
"ecr:StartImageScan",
"ecr:TagResource",
"ecr:UntagResource",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListClusters",
"events:PutRule",
"events:DescribeRule",
```



```
"events:PutTargets",
"events:TagResource",
"events:ListTagsForResource",
"fsx:DescribeFileSystems",
"glue:SearchTables",
"glue:NotifyEvent",
"glue:StartBlueprintRun",
"glue:PutWorkflowRunProperties",
"glue:StopCrawler",
"glue>DeleteJob",
"glue>DeleteWorkflow",
"glue:UpdateCrawler",
"glue>DeleteBlueprint",
"glue:UpdateWorkflow",
"glue:StartCrawler",
"glue:ResetJobBookmark",
"glue:UpdateJob",
"glue:StartWorkflowRun",
"glue:StopCrawlerSchedule",
"glue:ResumeWorkflowRun",
"glue>DeleteCrawler",
"glue:UpdateBlueprint",
"glue:BatchStopJobRun",
"glue:StopWorkflowRun",
"glue:BatchGet*",
"glue:UpdateCrawlerSchedule",
"glue>DeleteConnection",
"glue:UpdateConnection",
"glue:Get*",
"glue:BatchDeleteConnection",
"glue:StartCrawlerSchedule",
"glue:StartJobRun",
"glue:CreateWorkflow",
"glue:*DataQuality*",
"glue:List*",
"glue:CreateSession",
"glue:RunStatement",
"glue:BatchCreatePartition",
"glue:CreateDatabase",
"glue:CreatePartitionIndex",
"glue:CreateTable",
"glue:BatchUpdatePartition",
"glue:BatchDeletePartition",
"glue:UpdateTable",
```

```
"glue:DeleteTableVersion",
"glue:DeleteTable",
"glue:DeleteColumnStatisticsForPartition",
"glue:DeleteColumnStatisticsForTable",
"glue:DeletePartitionIndex",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"glue:BatchDeleteTableVersion",
"glue:BatchDeleteTable",
"glue:CreatePartition",
"glue:DeletePartition",
"glue:UpdatePartition",
"glue:CreateBlueprint",
"glue:CreateJob",
"glue:CreateConnection",
"glue:CreateCrawler",
"groundtruthlabeling:*",
"iam:CreateServiceLinkedRole",
"iam:GetRole",
"iam:ListRoles",
"iam:PassRole",
"kms:DescribeKey",
"kms:ListAliases",
"kms:Decrypt",
"kms:ListKeys",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:RetireGrant",
"lakeformation:GetDataAccess",
"lambda:ListFunctions",
"lambda:InvokeFunction",
"logs:CreateLogDelivery",
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:DeleteLogDelivery",
"logs:Describe*",
"logs:GetLogDelivery",
"logs:GetLogEvents",
"logs:ListLogDeliveries",
"logs:PutLogEvents",
"logs:UpdateLogDelivery",
"ram:AcceptResourceShareInvitation",
"rds:DescribeDBInstances",
"redshift:CreateClusterUser",
```

```
"redshift:GetClusterCredentials",
"redshift:GetClusterCredentialsWithIAM",
"redshift:DescribeClusters",
"redshift-data:BatchExecuteStatement",
"redshift-data:CancelStatement",
"redshift-data:DescribeStatement",
"redshift-data:DescribeTable",
"redshift-data:ExecuteStatement",
"redshift-data:GetStatementResult",
"redshift-data:ListSchemas",
"redshift-data:ListTables",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListWorkgroups",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:GetCredentials",
"s3:GetBucketAcl",
"s3:PutObjectAcl",
"s3:GetObject",
"s3:PutObject",
"s3>DeleteObject",
"s3:AbortMultipartUpload",
"s3:CreateBucket",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:ListAllMyBuckets",
"s3:GetBucketCors",
"s3:PutBucketCors",
"s3>DeleteObjectVersion",
"s3:PutObjectRetention",
"s3:ReplicateObject",
"s3:RestoreObject",
"secretsmanager:ListSecrets",
"secretsmanager:DescribeSecret",
"secretsmanager:GetSecretValue",
"secretsmanager:CreateSecret",
"secretsmanager:PutResourcePolicy",
"secretsmanager:TagResource",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:ProvisionProduct",
```

```
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneSageMakerManageAccessRolePolicy

説明：この AmazonDataZoneSageMakerManageAccessRolePolicy ポリシーは DataZone、SageMaker 環境内のさまざまなリソースへのアクセスをユーザーに許可するために必要なアクセス許可を Amazon に付与します。

AmazonDataZoneSageMakerManageAccessRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneSageMakerManageAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:34 UTC
- 編集日時: 2024 年 4 月 23 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerManageAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
```

```
"Action" : [
  "sagemaker:AddTags",
  "sagemaker:DeleteTags"
],
"Resource" : "*",
"Condition" : {
  "ForAnyValue:StringLike" : {
    "aws:TagKeys" : [
      "sagemaker:shared-with:*"
    ]
  }
}
},
{
  "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:PutModelPackageGroupPolicy",
    "sagemaker>DeleteModelPackageGroupPolicy"
  ],
  "Resource" : [
    "arn*:sagemaker:*:*:model-package-group/*"
  ]
},
{
  "Sid" : "AmazonSageMakerRAMPermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShares",
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:PutResourcePolicy",
    "sagemaker:GetResourcePolicy",
    "sagemaker>DeleteResourcePolicy"
  ],
  "Resource" : [
    "arn*:sagemaker:*:*:feature-group/*"
  ]
}
```

```
]
},
{
  "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:TagResource"
  ],
  "Resource" : "arn:*:ram:*:*:resource-share/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AwsDataZoneDomainId" : "false"
    }
  }
},
{
  "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:DeleteResourceShare"
  ],
  "Resource" : "arn:*:ram:*:*:resource-share/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AwsDataZoneDomainId" : "false"
    }
  }
},
{
  "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
  "Effect" : "Allow",
  "Action" : [
    "ram:CreateResourceShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLikeIfExists" : {
      "ram:RequestedResourceType" : [
        "sagemaker:*"
      ]
    }
  },
  "Null" : {
    "aws:RequestTag/AwsDataZoneDomainId" : "false"
  }
}
```

```
    }
  },
  {
    "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
    "Effect" : "Allow",
    "Action" : [
      "s3:DeleteBucketPolicy",
      "s3:PutBucketPolicy",
      "s3:GetBucketPolicy"
    ],
    "Resource" : [
      "arn:aws:s3:::sagemaker-datazone*",
      "arn:aws:s3:::SageMaker-DataZone*",
      "arn:aws:s3:::datazone-sagemaker*",
      "arn:aws:s3:::DataZone-SageMaker*",
      "arn:aws:s3:::amazon-datazone*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerS3Permission",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource" : [
      "arn:aws:s3:::sagemaker-datazone*",
      "arn:aws:s3:::SageMaker-DataZone*",
      "arn:aws:s3:::datazone-sagemaker*",
      "arn:aws:s3:::DataZone-SageMaker*",
      "arn:aws:s3:::amazon-datazone*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerECRPermission",
    "Effect" : "Allow",
    "Action" : [
      "ecr:GetRepositoryPolicy",
      "ecr:SetRepositoryPolicy",
      "ecr>DeleteRepositoryPolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
```



```
        "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
    }
}
},
{
    "Sid" : "AmazonSageMakerKMSReadPermission",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneEnvironment"
            ]
        }
    }
},
{
    "Sid" : "AmazonSageMakerKMSGrantPermission",
    "Effect" : "Allow",
    "Action" : [
        "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:TagKeys" : [
                "AmazonDataZoneEnvironment"
            ]
        },
        "ForAllValues:StringEquals" : {
            "kms:GrantOperations" : [
                "Decrypt"
            ]
        }
    }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDataZoneSageMakerProvisioningRolePolicy

説明：この AmazonDataZoneSageMakerProvisioningRolePolicy ポリシー DataZone は、Amazon と相互運用するために必要なアクセス許可を Amazon に付与します SageMaker。

AmazonDataZoneSageMakerProvisioningRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDataZoneSageMakerProvisioningRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 23 日 23:32 UTC
- 編集日時: 2024 年 4 月 23 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerProvisioningRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker>DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
    "aws:CalledViaFirst" : [
      "cloudformation.amazonaws.com"
    ]
  },
  "ForAnyValue:StringLike" : {
    "aws:TagKeys" : [
      "AmazonDataZoneEnvironment"
    ]
  },
  "Null" : {
    "aws:TagKeys" : "false",
    "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
  }
}
},
{
  "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:DescribeDomain"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
},
{
  "Sid" : "IamPassRolePermissions",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "glue.amazonaws.com",
        "lakeformation.amazonaws.com",

```

```
        "sagemaker.amazonaws.com"
    ],
    "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
    ]
}
},
{
    "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:CalledViaFirst" : [
                "cloudformation.amazonaws.com"
            ],
            "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
    }
},
{
    "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam>DeleteRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition" : {
        "StringEquals" : {
```

```
        "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
        ]
    }
}
},
{
    "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
    "Effect" : "Allow",
    "Action" : [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSserviceRoleForAmazonSageMakerNotebooks"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:CalledViaFirst" : [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
    "Effect" : "Allow",
    "Action" : [
        "kms:DescribeKey"
    ],
    "Resource" : "arn:aws:kms::*:key/*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
    }
}
```

```
    }
  }
},
{
  "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateConnection",
    "glue>DeleteConnection"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:CalledViaFirst" : [
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDetectiveFullAccess

説明： Amazon Detective サービスへのフルアクセスとコンソール UI の依存関係へのスコープ付きアクセスを提供します

AmazonDetectiveFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 30 日 17:57 UTC
- 編集日時: 2023 年 5 月 17 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDetectiveInvestigatorAccess

説明：調査員に Amazon Detective サービスへのアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。このポリシーでは、調査目的で Detective に掘り下げるアクセス許可と、Guardduty への制限付き書き込みアクセス許可を付与します。

AmazonDetectiveInvestigatorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveInvestigatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 17 日 15:24 UTC
- 編集日時: 2023 年 11 月 27 日 03:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDetectiveMemberAccess

説明： Amazon Detective サービスへのメンバーアクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。

AmazonDetectiveMemberAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveMemberAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 17 日 15:16 UTC
- 編集日時: 2023 年 1 月 17 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "detective:BatchGetMembershipDatasesources",
    "detective:DisassociateMembership",
    "detective:GetFreeTrialEligibility",
    "detective:GetPricingInformation",
    "detective:GetUsageInformation",
    "detective:ListInvitations",
    "detective:RejectInvitation"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDetectiveOrganizationsAccess

説明： Amazon Detective の委任された管理者を管理するための Organizations アクセスと、コンソール UI の依存関係へのスコープ付きアクセスを提供します。これにより、Detective のサービスリンクロールを作成するアクセス許可も付与されます。

AmazonDetectiveOrganizationsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDetectiveOrganizationsAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 2 日 15:20 UTC
- 編集日時: 2023 年 3 月 2 日 15:20 UTC

- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDetectiveServiceLinkedRolePolicy

説明 : Amazon Detective がユーザーに代わってサービスコールを実行することを許可する

AmazonDetectiveServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 18 日 19:47 UTC
- 編集日時: 2021 年 11 月 18 日 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
{
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDevOpsGuruConsoleFullAccess

説明: ポリシーは、DevOps Guru コンソールへのフルアクセスを許可します。

AmazonDevOpsGuruConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 12 月 17 日 18:43 UTC
- 編集日時: 2022 年 8 月 25 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDevOpsGuruFullAccess

説明： Amazon DevOps Guru へのフルアクセスを提供します。

AmazonDevOpsGuruFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:38 UTC
- 編集日時: 2022 年 8 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDevOpsGuruOrganizationsAccess

説明：組織内で Amazon DevOps Guru を有効化および管理するためのアクセスを提供します。

AmazonDevOpsGuruOrganizationsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 15 日 23:50 UTC
- 編集日時: 2021 年 11 月 15 日 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDevOpsGuruReadOnlyAccess

説明： Amazon DevOps Guru コンソールへの読み取り専用アクセスを提供します。

AmazonDevOpsGuruReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDevOpsGuruReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:34 UTC
- 編集日時: 2022 年 8 月 25 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDevOpsGuruServiceRolePolicy

説明： Amazon が リソースにアクセス DevOpsGuru するために必要なサービスにリンクされたロール。

AmazonDevOpsGuruServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 1 日 10:24 UTC
- 編集日時: 2023 年 1 月 10 日 14:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDMSCloudWatchLogsRole

説明：DMS レプリケーションログをお客様のアカウントの cloudwatch ログにアップロードするためのアクセスを提供します。

AmazonDMSCloudWatchLogsRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSCloudWatchLogsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 7 日 23:44 UTC
- 編集日時: 2023 年 5 月 23 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDMSRedshiftS3Role

説明：DMS の Redshift エンドポイントの S3 設定を管理するためのアクセスを提供します。

AmazonDMSRedshiftS3Role は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSRedshiftS3Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 20 日 17:05 UTC
- 編集日時: 2019 年 7 月 8 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDMSVPCManagementRole

説明 : AWS マネージドカスタマー設定の VPC 設定を管理するためのアクセスを提供します

AmazonDMSVPCManagementRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDMSVPCManagementRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 18 日 16:33 UTC
- 編集日時: 2016 年 5 月 23 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDB-ElasticServiceRolePolicy

説明 : Amazon DocumentDB -Elastic がユーザーに代わって AWS リソースを管理できるようにします。

AmazonDocDB-ElasticServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 14:17 UTC
- 編集日時: 2022 年 11 月 30 日 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDBConsoleFullAccess

説明： を使用して MongoDB 互換の Amazon DocumentDB を管理するためのフルアクセスを提供します AWS Management Console。 MongoDB このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスと VPC 設定を作成および編集するアクセス許可、Amazon KMS でキーを表示および一覧表示するアクセス許可、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

AmazonDocDBConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:37 UTC
- 編集日時: 2022 年 11 月 30 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic>DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic>DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds>DeleteDBCluster",
        "rds>DeleteDBClusterParameterGroup",
        "rds>DeleteDBClusterSnapshot",
        "rds>DeleteDBInstance",
        "rds>DeleteDBParameterGroup",
        "rds>DeleteDBSubnetGroup",
        "rds>DeleteEventSubscription",
```

```
"rds:DeleteGlobalCluster",
"rds:DescribeAccountAttributes",
"rds:DescribeCertificates",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusterSnapshotAttributes",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBLogFiles",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultClusterParameters",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEventCategories",
"rds:DescribeEventSubscriptions",
"rds:DescribeEvents",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribePendingMaintenanceActions",
"rds:DescribeValidDBInstanceModifications",
"rds:DownloadDBLogFilePortion",
"rds:FailoverDBCluster",
"rds:ListTagsForResource",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterParameterGroup",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
"rds:ModifyDBSubnetGroup",
"rds:ModifyEventSubscription",
"rds:ModifyGlobalCluster",
"rds:PromoteReadReplicaDBCluster",
"rds:RebootDBInstance",
"rds:RemoveFromGlobalCluster",
"rds:RemoveRoleFromDBCluster",
"rds:RemoveSourceIdentifierFromSubscription",
"rds:RemoveTagsFromResource",
"rds:ResetDBClusterParameterGroup",
"rds:ResetDBParameterGroup",
```

```
    "rds:RestoreDBClusterFromSnapshot",
    "rds:RestoreDBClusterToPointInTime"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "ec2:AllocateAddress",
    "ec2:AssignIpv6Addresses",
    "ec2:AssignPrivateIpAddresses",
    "ec2:AssociateAddress",
    "ec2:AssociateRouteTable",
    "ec2:AssociateSubnetCidrBlock",
    "ec2:AssociateVpcCidrBlock",
    "ec2:AttachInternetGateway",
    "ec2:AttachNetworkInterface",
    "ec2:CreateCustomerGateway",
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc",
    "ec2:CreateInternetGateway",
    "ec2:CreateNatGateway",
    "ec2:CreateNetworkInterface",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSubnet",
    "ec2:CreateVpc",
    "ec2:CreateVpcEndpoint",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRouteTables",
```

```

    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:ModifyVpcEndpoint",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "kms:ListRetirableGrants",
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "sns:ListSubscriptions",
    "sns:ListTopics",
    "sns:Publish"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "rds.amazonaws.com"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
    }
  }
}

```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDBElasticFullAccess

説明: Amazon DocumentDB Elastic クラスターへのフルアクセスと、EC2、KMS SecretsManager、CloudWatch IAM などの依存関係に必要なその他のアクセス許可を提供します。

AmazonDocDBElasticFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 5 日 13:51 UTC
- 編集日時: 2023 年 6 月 21 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDBElasticReadOnlyAccess

説明： Amazon DocDB -Elastic および CloudWatch メトリクスへの読み取り専用アクセスを提供します。

AmazonDocDBElasticReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBElasticReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 8 日 14:37 UTC
- 編集日時: 2023 年 6 月 21 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDBFullAccess

説明： MongoDB との互換性を持つ Amazon DocumentDB へのフルアクセスを提供します。MongoDB このポリシーは、アカウント内のすべての SNS トピックを公開するためのフルアクセスと、Amazon RDS と Amazon Neptune へのフルアクセス権も付与します。

AmazonDocDBFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:21 UTC
- 編集日時: 2019 年 1 月 9 日 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDocDBReadOnlyAccess

説明： MongoDB との互換性を持つ Amazon DocumentDB への読み取り専用アクセスを提供します。 MongoDB このポリシーは Amazon RDS と Amazon Neptune リソースへのアクセス権も付与します。

AmazonDocDBReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDocDBReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 9 日 20:30 UTC
- 編集日時: 2019 年 1 月 9 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDRSVPCManagement

説明： Amazon マネージドカスタマー設定の VPC 設定を管理するためのアクセスを提供します

AmazonDRSVPCManagement は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDRSVPCManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 9 月 2 日 00:09 UTC
- 編集日時: 2015 年 9 月 2 日 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDynamoDBFullAccess

説明： 経由で Amazon DynamoDB へのフルアクセスを提供します AWS Management Console。

AmazonDynamoDBFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 1 月 29 日 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonDynamoDBFullAccesswithDataPipeline

説明：このポリシーは非推奨パスにあります。ガイダンスについては、「<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>」のドキュメントを参照してください。経由で AWS Data Pipeline を使用したエクスポート/インポートを含む Amazon DynamoDB へのフルアクセスを提供します AWS Management Console。

AmazonDynamoDBFullAccesswithDataPipeline は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBFullAccesswithDataPipeline をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 11 月 12 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonDynamoDBReadOnlyAccess

説明： 経由で Amazon DynamoDB への読み取り専用アクセスを提供します AWS Management Console。

AmazonDynamoDBReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonDynamoDBReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 3 月 20 日 15:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEBSCSIDriverPolicy

説明：CSI ドライバーサービスアカウントがユーザーに代わって EC2 などの関連サービスを呼び出すことを許可する IAM ポリシー。

AmazonEBSCSIDriverPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEBSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 17:24 UTC
- 編集日時: 2022 年 11 月 18 日 14:42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerRegistryFullAccess

説明： Amazon ECR リソースへの管理アクセスを提供します

AmazonEC2ContainerRegistryFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:06 UTC
- 編集日時: 2020 年 12 月 5 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerRegistryPowerUser

説明: Amazon EC2 Container Registry リポジトリへのフルアクセスを提供しますが、リポジトリの削除やポリシーの変更は許可しません。

AmazonEC2ContainerRegistryPowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:05 UTC
- 編集日時: 2019 年 12 月 10 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerRegistryReadOnly

説明： Amazon EC2 Container Registry リポジトリへの読み取り専用アクセスを提供します。

AmazonEC2ContainerRegistryReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerRegistryReadOnly をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 21 日 17:04 UTC
- 編集日時: 2019 年 12 月 10 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerServiceAutoscaleRole

説明： Amazon EC2 Container Service のタスクの自動スケーリングを有効にするポリシー

AmazonEC2ContainerServiceAutoscaleRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 5 月 12 日 23:25 UTC
- 編集日時: 2018 年 2 月 5 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeServices",
      "ecs:UpdateService"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms",
      "cloudwatch:PutMetricAlarm"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerServiceEventsRole

説明 : EC2 Container Service の CloudWatch イベントを有効にするポリシー

AmazonEC2ContainerServiceEventsRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceEventsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 5 月 30 日 16:51 UTC
- 編集日時: 2023 年 3 月 6 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerServiceforEC2Role

説明： Amazon EC2 Container Service の Amazon EC2 ロールのデフォルトポリシー。

AmazonEC2ContainerServiceforEC2Role は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceforEC2Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 3 月 19 日 18:45 UTC
- 編集日時: 2023 年 3 月 6 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ContainerServiceRole

説明： Amazon ECS サービスロールのデフォルトポリシー。

AmazonEC2ContainerServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ContainerServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 16:14 UTC

- 編集日時: 2016 年 8 月 11 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2FullAccess

説明： 経由で Amazon EC2 へのフルアクセスを提供します AWS Management Console。

AmazonEC2FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 11 月 27 日 02:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2ReadOnlyAccess

説明： 経由で Amazon EC2 への読み取り専用アクセスを提供します AWS Management Console。

AmazonEC2ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 2 月 14 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2RoleforAWSCodeDeploy

説明： リビジョンをダウンロードするための S3 バケットへの EC2 アクセスを提供します。このロールは EC2 インスタンスの CodeDeploy エージェントが必要とするものです。

AmazonEC2RoleforAWSCodeDeploy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforAWSCodeDeploy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 19 日 18:10 UTC
- 編集日時: 2017 年 3 月 20 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2RoleforAWSCodeDeployLimited

説明 : EC2 に S3 バケットへの制限付きアクセスを提供し、リビジョンをダウンロードします。このロールは EC2 インスタンスの CodeDeploy エージェントが必要とするものです。

AmazonEC2RoleforAWSCodeDeployLimited は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforAWSCodeDeployLimited をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 24 日 17:55 UTC
- 編集日時: 2022 年 1 月 20 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2RoleforDataPipelineRole

説明 : Data Pipeline サービスロールの Amazon EC2 ロールのデフォルトポリシー。

AmazonEC2RoleforDataPipelineRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforDataPipelineRole をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2016 年 2 月 22 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2RoleforSSM

説明: このポリシーは間もなく廃止されます。EC2 インスタンスで AWS Systems Manager サービスコア機能を有効にするには、AmazonSSMManagedInstanceCore ポリシーを使用してください。詳細については、<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html> を参照してください。

AmazonEC2RoleforSSM は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RoleforSSM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 29 日 17:48 UTC
- 編集日時: 2019 年 1 月 24 日 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2RolePolicyForLaunchWizard

説明： EC2 の Amazon LaunchWizard サービスロールの マネージドポリシー

AmazonEC2RolePolicyForLaunchWizard は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2RolePolicyForLaunchWizard をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 08:05 UTC
- 編集日時: 2022 年 5 月 16 日 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

ポリシーのバージョニング

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2SpotFleetAutoscaleRole

説明： Amazon EC2 スポットフリートの自動スケーリングを有効にするポリシー

AmazonEC2SpotFleetAutoscaleRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetAutoscaleRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 8 月 19 日 18:27 UTC
- 編集日時: 2019 年 2 月 18 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEC2SpotFleetTaggingRole

説明： EC2 スポットフリートがユーザーに代わってスポットインスタンスをリクエスト、終了、タグ付けできるようにします。

AmazonEC2SpotFleetTaggingRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEC2SpotFleetTaggingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 29 日 18:19 UTC
- 編集日時: 2020 年 4 月 23 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonECS_FullAccess

説明: Amazon ECS リソースへの管理アクセスを提供し、VPCs、CloudFormation スタックなどの他の AWS サービスリソースへのアクセスを通じて ECS 機能を有効にします。Auto Scaling

AmazonECS_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECS_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 7 日 21:36 UTC
- 編集日時: 2023 年 1 月 4 日 16:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v20 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

説明: プライベート認証機関、AWS Secrets Manager、およびユーザーに代わって ECS Service Connect TLS 機能を管理する AWS のサービスのために必要なその他のへの管理アクセスを提供します。

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 19 日 20:08 UTC
- 編集日時: 2024 年 1 月 19 日 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
```

```
"Effect" : "Allow",
"Action" : [
  "secretsmanager:DescribeSecret",
  "secretsmanager:UpdateSecret",
  "secretsmanager:GetSecretValue",
  "secretsmanager:PutSecretValue",
  "secretsmanager>DeleteSecret",
  "secretsmanager:RotateSecret",
  "secretsmanager:UpdateSecretVersionStage"
],
"Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
"Condition" : {
  "StringEquals" : {
    "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "ManagePrivateCertificateAuthority",
  "Effect" : "Allow",
  "Action" : [
    "acm-pca:GetCertificate",
    "acm-pca:GetCertificateAuthorityCertificate",
    "acm-pca:DescribeCertificateAuthority"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSTags" : "true"
    }
  }
},
{
  "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
  "Effect" : "Allow",
  "Action" : [
    "acm-pca:IssueCertificate"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSTags" : "true",
      "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
    }
  }
}
```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonECSInfrastructureRolePolicyForVolumes

説明： ECS ワークロードに関連付けられたボリュームをユーザーに代わって管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

AmazonECSInfrastructureRolePolicyForVolumes は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSInfrastructureRolePolicyForVolumes をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 10 日 22:56 UTC
- 編集日時: 2024 年 1 月 10 日 22:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
```

```
    "ec2:DescribeAvailabilityZones"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ManageEBSVolumeLifecycle",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
},
{
  "Sid" : "ManageVolumeAttachmentsForEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*"
},
{
  "Sid" : "DeleteEBSManagedVolume",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteVolume",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "ArnLike" : {
      "aws:ResourceTag/AmazonECSManaged" : "arn:aws:ecs:*:*:task/*"
    },
    "StringEquals" : {
      "aws:ResourceTag/AmazonECSManaged" : "true"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonECSServiceRolePolicy

説明: Amazon ECS がクラスターを管理できるようにするポリシー。

AmazonECSServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 14 日 01:18 UTC
- 編集日時: 2023 年 12 月 4 日 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonECSTaskExecutionRolePolicy

説明： Amazon ECS タスクの実行に必要な他の AWS サービスリソースへのアクセスを提供します

AmazonECSTaskExecutionRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonECSTaskExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 16 日 18:48 UTC
- 編集日時: 2017 年 11 月 16 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEFSCSIDriverPolicy

説明： EFS リソースへの管理アクセスと EC2 への読み取りアクセスを提供します

AmazonEFSCSIDriverPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEFSCSIDriverPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 7 月 25 日 20:10 UTC
- 編集日時: 2023 年 7 月 25 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEKS_CNI_Policy

説明: このポリシーは、EKS ワーカーノードの IP アドレス設定を変更するために必要なアクセス許可を Amazon VPC CNI プラグイン (amazon-vpc-cni-k8s) に提供します。このアクセス許可セットにより、CNI はユーザーに代わって Elastic Network Interface の一覧表示、説明、変更を行うことができます。AWS VPC CNI プラグインの詳細については、<https://github.com/aws/amazon-vpc-cni-k8s> を参照してください。

AmazonEKS_CNI_Policy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKS_CNI_Policy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:07 UTC
- 編集日時: 2024 年 3 月 4 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSClusterPolicy

説明：このポリシーは、ユーザーに代わってリソースを管理するために必要なアクセス許可を Kubernetes に提供します。Kubernetes では `Ec2EC2:CreateTags permissions` が必要です。

AmazonEKSClusterPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:06 UTC
- 編集日時: 2023 年 2 月 7 日 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSCoordinatorServiceRolePolicy

説明： このポリシーは、Amazon EKS が EKS コネクタの AWS リソースを管理することを許可します。

AmazonEKSCoordinatorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 4 日 20:31 UTC
- 編集日時: 2021 年 9 月 4 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSCoordinatorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm>DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*:*:document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
```

```
"Action" : [
  "iam:PassRole"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "ssm.amazonaws.com"
    ]
  }
},
{
  "Sid" : "PutManagedEventRule",
  "Effect" : "Allow",
  "Action" : "events:PutRule",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "eks-connector.amazonaws.com",
      "events:source" : "aws.ssm"
    }
  }
},
{
  "Sid" : "PutManagedEventTarget",
  "Effect" : "Allow",
  "Action" : "events:PutTargets",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "events:ManagedBy" : "eks-connector.amazonaws.com"
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSFargatePodExecutionRolePolicy

説明： AWS Fargate で Amazon EKS ポッドを実行するために必要な他の AWS サービスリソースへのアクセスを提供します

AmazonEKSFargatePodExecutionRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSFargatePodExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 22 日 04:34 UTC
- 編集日時: 2019 年 11 月 22 日 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ]
    }
  ]
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSFargateServiceRolePolicy

説明： このポリシーは、Amazon EKS に Fargate タスクを実行するために必要なアクセス許可を付与します。

AmazonEKSFargateServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 22 日 04:36 UTC
- 編集日時: 2019 年 11 月 22 日 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSLocalOutpostClusterPolicy

説明: このポリシーは、アカウントで実行されている EKS ローカルクラスターのコントロールプレーンインスタンスに、ユーザーに代わって リソースを管理するためのアクセス許可を提供します。

AmazonEKSLocalOutpostClusterPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSLocalOutpostClusterPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 24 日 21:56 UTC
- 編集日時: 2022 年 10 月 17 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSLocalOutpostServiceRolePolicy

説明： Amazon EKS Local がユーザーに代わって AWS サービスを呼び出すことを許可します。

AmazonEKSLocalOutpostServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 8 月 23 日 21:53 UTC
- 編集日時: 2022 年 10 月 24 日 16:24 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSServicePolicy

説明： このポリシーにより、Amazon Elastic Container Service for Kubernetes は EKS クラスターを運用するために必要なリソースを作成および管理できます。

AmazonEKSServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSServicePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:08 UTC
- 編集日時: 2020 年 5 月 27 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSServiceRolePolicy

説明: Amazon EKS がユーザーに代わって サービスを呼び出すために必要な AWS サービスにリンクされたロール。

AmazonEKSServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 2 月 21 日 20:10 UTC
- 編集日時: 2020 年 5 月 27 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSVPCResourceController

説明： VPC リソースコントローラーがワーカーノードの ENI と IPs を管理するために使用されるポリシー。

AmazonEKSVPCResourceController は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSVPCResourceController をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 12 日 00:55 UTC

- 編集日時: 2020 年 8 月 12 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEKSWorkerNodePolicy

説明：このポリシーは、Amazon EKS ワーカーノードが Amazon EKS クラスターに接続することを許可します。

AmazonEKSWorkerNodePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEKSWorkerNodePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 27 日 21:09 UTC
- 編集日時: 2023 年 11 月 27 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElastiCacheFullAccess

説明 : ElastiCache 経由で Amazon へのフルアクセスを提供します AWS Management Console。

AmazonElastiCacheFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElastiCacheFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 11 月 28 日 03:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
```

```
"Effect" : "Allow",
"Action" : "ec2:CreateVpcEndpoint",
"Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
"Condition" : {
  "StringLike" : {
    "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
  }
},
{
  "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint"
  ],
  "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
},
{
  "Sid" : "TagVPCEndpointsOnCreation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint",
      "aws:RequestTag/AmazonElastiCacheManaged" : "true"
    }
  }
},
{
  "Sid" : "AllowAccessToEc2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowAccessToKMS",
  "Effect" : "Allow",
```

```
"Action" : [
  "kms:DescribeKey",
  "kms:ListAliases",
  "kms:ListKeys"
],
"Resource" : "*"
},
{
  "Sid" : "AllowAccessToCloudWatch",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricData"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowAccessToAutoScaling",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScalingActivities"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeLogGroups",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListLogDeliveryStreams",
  "Effect" : "Allow",
  "Action" : [
    "firehose:ListDeliveryStreams"
  ],
  "Resource" : "*"
},
{
```

```
    "Sid" : "DescribeS3Buckets",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAccessToOutposts",
    "Effect" : "Allow",
    "Action" : [
      "outposts:ListOutposts"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowAccessToSNS",
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElastiCacheReadOnlyAccess

説明：ElastiCache 経由で Amazon への読み取り専用アクセスを提供します AWS Management Console。

AmazonElastiCacheReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElastiCacheReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticContainerRegistryPublicFullAccess

説明： Amazon ECR Public リソースへの管理アクセスを提供します

AmazonElasticContainerRegistryPublicFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 17:25 UTC
- 編集日時: 2020 年 12 月 1 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "ecr-public:*",
    "sts:GetServiceBearerToken"
  ],
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticContainerRegistryPublicPowerUser

説明: Amazon ECR Public リポジトリへのフルアクセスを提供しますが、リポジトリの削除やポリシーの変更は許可しません。

AmazonElasticContainerRegistryPublicPowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:16 UTC
- 編集日時: 2020 年 12 月 1 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicPowerUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticContainerRegistryPublicReadOnly

説明： Amazon ECR Public リポジトリへの読み取り専用アクセスを提供します。

AmazonElasticContainerRegistryPublicReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticContainerRegistryPublicReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 17:27 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemClientFullAccess

説明 : Amazon EFS ファイルシステムへのルートクライアントアクセスを提供します

AmazonElasticFileSystemClientFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:27 UTC
- 編集日時: 2020 年 1 月 13 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemClientReadOnlyAccess

説明 : Amazon EFS ファイルシステムへの読み取り専用クライアントアクセスを提供します

AmazonElasticFileSystemClientReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:24 UTC
- 編集日時: 2020 年 1 月 13 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemClientReadWriteAccess

説明： Amazon EFS ファイルシステムへの読み取りおよび書き込みクライアントアクセスを提供します。

AmazonElasticFileSystemClientReadWriteAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemClientReadWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 13 日 16:21 UTC
- 編集日時: 2020 年 1 月 13 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "elasticfilesystem:ClientMount",
  "elasticfilesystem:ClientWrite",
  "elasticfilesystem:DescribeMountTargets"
],
"Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemFullAccess

説明： 経由で Amazon EFS へのフルアクセスを提供します AWS Management Console。

AmazonElasticFileSystemFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 27 日 16:22 UTC
- 編集日時: 2023 年 11 月 28 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemReadOnlyAccess

説明： 経由で Amazon EFS への読み取り専用アクセスを提供します AWS Management Console。

AmazonElasticFileSystemReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 27 日 16:25 UTC
- 編集日時: 2022 年 1 月 10 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemServiceRolePolicy

説明： Amazon Elastic File System がユーザーに代わって AWS リソースを管理することを許可する

AmazonElasticFileSystemServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:52 UTC
- 編集日時: 2022 年 1 月 10 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticFileSystemsUtils

説明 : AWS Systems Manager を使用して EC2 インスタンスで Amazon EFS ユーティリティ (amazon-efs-utils) パッケージを自動的に管理し、 CloudWatchLog を使用して EFS ファイルシステムのマウントの成功/失敗通知を取得できるようにします。

AmazonElasticFileSystemsUtils は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticFileSystemsUtils をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 9 月 29 日 15:16 UTC
- 編集日時: 2020 年 9 月 29 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceEditorsRole

説明： Amazon Elastic MapReduce Editors サービスロールのデフォルトポリシー。

AmazonElasticMapReduceEditorsRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceEditorsRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 16 日 21:55 UTC
- 編集日時: 2023 年 2 月 9 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceforAutoScalingRole

説明： Amazon Elastic MapReduce for Auto Scaling 。 Auto Scaling が EMR クラスターにインスタンスを追加および削除できるようにするロールです。

AmazonElasticMapReduceforAutoScalingRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceforAutoScalingRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 18 日 01:09 UTC
- 編集日時: 2016 年 11 月 18 日 01:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceforEC2Role

説明： Amazon Elastic for EC2 サービスロール MapReduce のデフォルトポリシー。

AmazonElasticMapReduceforEC2Role は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceforEC2Role をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC

- 編集日時: 2017 年 8 月 11 日 23:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceFullAccess

説明：このポリシーは非推奨パスにあります。ガイダンスについては、ドキュメントを参照してください: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。EC2 MapReduce や S3 など、必要な Amazon Elastic および基盤となるサービスへのフルアクセスを提供します。

AmazonElasticMapReduceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 10 月 11 日 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReducePlacementGroupPolicy

説明： EMR が EC2 プレイスメントグループを作成、説明、削除できるようにするポリシー。

AmazonElasticMapReducePlacementGroupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReducePlacementGroupPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 29 日 00:37 UTC
- 編集日時: 2020 年 9 月 29 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceReadOnlyAccess

説明： MapReduce 経由で Amazon Elastic への読み取り専用アクセスを提供します AWS Management Console。

AmazonElasticMapReduceReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 7 月 29 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticMapReduceRole

説明：このポリシーは非推奨パスにあります。ガイダンスについては、ドキュメントを参照してください: <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。Amazon Elastic MapReduce サービスロールのデフォルトポリシー。

AmazonElasticMapReduceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticMapReduceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2020 年 6 月 24 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticsearchServiceRolePolicy

説明： Amazon Elasticsearch Service がユーザーに代わって EC2 Networking APIsなどの他の AWS サービスにアクセスできるようにします。

AmazonElasticsearchServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 7 月 7 日 00:15 UTC
- 編集日時: 2023 年 10 月 23 日 06:58 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticTranscoder_FullAccess

説明： Elastic Transcoder へのフルアクセスと、Elastic Transcoder のフル機能に必要な関連サービスへのアクセスをユーザーに許可します。

AmazonElasticTranscoder_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 27 日 18:59 UTC
- 編集日時: 2019 年 6 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticTranscoder_JobsSubmitter

説明：プリセットの変更、ジョブの送信、Elastic Transcoder 設定の表示を行うアクセス許可をユーザーに付与します。このポリシーでは、S3、IAM、SNS など、Elastic Transcode コンソールの使用に必要なその他のサービスへの読み取り専用アクセスも一部付与されます。

AmazonElasticTranscoder_JobsSubmitter は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_JobsSubmitter をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 7 日 21:12 UTC
- 編集日時: 2019 年 6 月 10 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticTranscoder_ReadOnlyAccess

説明： Elastic Transcoder への読み取り専用アクセスと、関連サービスへのリストアクセスをユーザーに許可します。

AmazonElasticTranscoder_ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoder_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 7 日 21:09 UTC
- 編集日時: 2019 年 6 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonElasticTranscoderRole

説明 : Amazon Elastic Transcoder サービスロールのデフォルトポリシー。

AmazonElasticTranscoderRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonElasticTranscoderRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 6 月 13 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRCleanupPolicy

説明： EMR サービスロールがその機能を失った場合に、EMR が AWS EC2 リソースを終了および削除するために必要なアクションを許可します。

AmazonEMRCleanupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 26 日 23:54 UTC
- 編集日時: 2020 年 9 月 29 日 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

ポリシーのバージョニング

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRContainersServiceRolePolicy

説明： Amazon EMR の実行に必要な他の AWS サービスリソースへのアクセスを許可します

AmazonEMRContainersServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 9 日 00:38 UTC
- 編集日時: 2023 年 3 月 10 日 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRFullAccessPolicy_v2

説明： Amazon EMR へのフルアクセスを提供します

AmazonEMRFullAccessPolicy_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRFullAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 12 日 01:50 UTC
- 編集日時: 2023 年 7 月 28 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRReadOnlyAccessPolicy_v2

説明： Amazon EMR および関連する CloudWatch メトリクスへの読み取り専用アクセスを提供します。

AmazonEMRReadOnlyAccessPolicy_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRReadOnlyAccessPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 12 日 01:39 UTC
- 編集日時: 2023 年 8 月 2 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRServerlessServiceRolePolicy

説明： Amazon EMRServerless の実行に必要な他の AWS サービスリソースへのアクセスを許可します

AmazonEMRServerlessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 20 日 23:15 UTC
- 編集日時: 2024 年 1 月 25 日 18:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEMRServicePolicy_v2

説明：このポリシーは Amazon EMR サービスロールに使用されるため、アカウントの他の IAM ユーザーまたはロールには使用しないでください。このポリシーは、EMR クラスターのオペレーションに必要な EMR および関連サービスに関連するリソースを作成および管理するためのアクセス許可を付与します。

AmazonEMRServicePolicy_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEMRServicePolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 3 月 12 日 01:11 UTC
- 編集日時: 2024 年 5 月 2 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
}
},
{
    "Sid" : "CreateWithEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "CreateEMRTaggedLaunchTemplate",
    "Effect" : "Allow",
    "Action" : "ec2:CreateLaunchTemplate",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
},
{
    "Sid" : "CreateEMRTaggedInstancesAndVolumes",
    "Effect" : "Allow",
    "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
    }
}
```

```
    }
  }
},
{
  "Sid" : "ResourcesToLaunchEC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:CreateFleet",
    "ec2:CreateLaunchTemplate",
    "ec2:CreateLaunchTemplateVersion"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/ami-*",
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:capacity-reservation/*",
    "arn:aws:ec2:*:*:placement-group/EMR_*",
    "arn:aws:ec2:*:*:fleet/*",
    "arn:aws:ec2:*:*:dedicated-host/*",
    "arn:aws:resource-groups:*:*:group/*"
  ]
},
{
  "Sid" : "ManageEMRTaggedResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplateVersion",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyInstanceAttribute",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "ManageTagsOnEMRTaggedResources",
  "Effect" : "Allow",
  "Action" : [
```

```
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
    }
  }
},
{
  "Sid" : "TagOnCreateTaggedEMRResources",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "StringEquals" : {
```

```
        "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
        ]
    }
},
{
    "Sid" : "TagPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateTags",
        "ec2>DeleteTags"
    ],
    "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
    ]
},
{
    "Sid" : "ListActionsForEC2Resources",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
    ],
    "Resource" : "*"
}
```



```
  },
  {
    "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:vpc/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
        "ec2:CreateAction" : "CreateSecurityGroup"
      }
    }
  }
}
```

```
  },
  {
    "Sid" : "ManageSecurityGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
      }
    }
  },
  {
    "Sid" : "CreateEMRPlacementGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreatePlacementGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
  },
  {
    "Sid" : "DeletePlacementGroups",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeletePlacementGroup"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AutoScaling",
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DeleteScalingPolicy",
      "application-autoscaling:DeregisterScalableTarget",
      "application-autoscaling:DescribeScalableTargets",
      "application-autoscaling:DescribeScalingPolicies",
      "application-autoscaling:PutScalingPolicy",
      "application-autoscaling:RegisterScalableTarget"
    ],
  },
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "ResourceGroupsForCapacityReservations",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AutoScalingCloudWatch",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricAlarm",
      "cloudwatch>DeleteAlarms",
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
  },
  {
    "Sid" : "PassRoleForAutoScaling",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
      }
    }
  },
  {
    "Sid" : "PassRoleForEC2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com*"
      }
    }
  }
]
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonESCognitoAccess

説明： Amazon Cognito 設定サービスへの制限付きアクセスを提供します。

AmazonESCognitoAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 28 日 22:29 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonESFullAccess

説明： Amazon ES 設定サービスへのフルアクセスを提供します。

AmazonESFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 1 日 19:14 UTC
- 編集日時: 2015 年 10 月 1 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonESReadOnlyAccess

説明： Amazon ES 設定サービスへの読み取り専用アクセスを提供します。

AmazonESReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonESReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 1 日 19:18 UTC
- 編集日時: 2018 年 10 月 3 日 03:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Action" : [
    "es:Describe*",
    "es:List*",
    "es:Get*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

説明： EventBridge がユーザーに代わって Secret Manager リソースにアクセスできるようにします。

AmazonEventBridgeApiDestinationsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 11 日 20:52 UTC
- 編集日時: 2021 年 2 月 11 日 20:52 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeFullAccess

説明 : Amazon へのフルアクセスを提供します EventBridge。

AmazonEventBridgeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 11 日 14:08 UTC
- 編集日時: 2022 年 12 月 1 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgePipesFullAccess

説明 : Amazon EventBridge Pipes へのフルアクセスを提供します。

AmazonEventBridgePipesFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgePipesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:03 UTC
- 編集日時: 2022 年 12 月 1 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgePipesOperatorAccess

説明： Amazon EventBridge Pipes への読み取り専用アクセスとオペレーター (パイプの実行を停止および開始する機能) アクセスを提供します。

AmazonEventBridgePipesOperatorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgePipesOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgePipesReadOnlyAccess

説明： Amazon EventBridge Pipes への読み取り専用アクセスを提供します。

AmazonEventBridgePipesReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgePipesReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 12 月 1 日 17:04 UTC
- 編集日時: 2022 年 12 月 1 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeReadOnlyAccess

説明： Amazon への読み取り専用アクセスを提供します EventBridge。

AmazonEventBridgeReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 11 日 13:59 UTC
- 編集日時: 2022 年 12 月 1 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeSchedulerFullAccess

説明: AmazonEventBridgeSchedulerFullAccess マネージドポリシーは、スケジュールとスケジュールグループに対してすべての Amazon EventBridge クレジットアクションを使用するアクセス許可を付与します。

AmazonEventBridgeSchedulerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchedulerFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 18:37 UTC
- 編集日時: 2022 年 11 月 10 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeSchedulerReadOnlyAccess

説明: AmazonEventBridgeSchedulerReadOnlyAccess 管理ポリシーは、スケジュールとスケジュールグループの詳細を表示する読み取り専用アクセス許可を付与します。

AmazonEventBridgeSchedulerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonEventBridgeSchedulerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 18:50 UTC
- 編集日時: 2022 年 11 月 10 日 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeSchemasFullAccess

説明： Amazon EventBridge Schemas へのフルアクセスを提供します。

AmazonEventBridgeSchemasFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchemasFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 28 日 23:12 UTC
- 編集日時: 2019 年 11 月 28 日 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeSchemasReadOnlyAccess

説明： Amazon EventBridge Schemas への読み取り専用アクセスを提供します。

AmazonEventBridgeSchemasReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonEventBridgeSchemasReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 28 日 23:05 UTC
- 編集日時: 2020 年 5 月 1 日 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonEventBridgeSchemasServiceRolePolicy

説明: Amazon EventBridge スキーマによって作成された マネージドルールにアクセス許可を付与します。

AmazonEventBridgeSchemasServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2019 年 11 月 27 日 01:10 UTC
- 編集日時: 2019 年 11 月 27 日 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonFISServiceRolePolicy

説明: AWS FIS が実験のモニタリングとリソース選択を管理できるようにするポリシー。

AmazonFISServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:18 UTC
- 編集日時: 2022 年 10 月 25 日 09:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonForecastFullAccess

説明： Amazon Forecast のすべてのアクションへのアクセスを許可します

AmazonForecastFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonForecastFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 01:52 UTC
- 編集日時: 2019 年 1 月 18 日 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonFraudDetectorFullAccessPolicy

説明： Amazon Fraud Detector のすべてのアクションへのアクセスを許可します

AmazonFraudDetectorFullAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFraudDetectorFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 22:46 UTC
- 編集日時: 2019 年 12 月 3 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonFreeRTOSFullAccess

説明： Amazon FreeRTOS のフルアクセスポリシー

AmazonFreeRTOSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFreeRTOSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 15:32 UTC
- 編集日時: 2017 年 11 月 29 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonFreeRTOSOTAUpdate

説明：ユーザーに Amazon FreeRTOS OTA 更新へのアクセスを許可する

AmazonFreeRTOSOTAUpdate は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFreeRTOSOTAUpdate をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 8 月 27 日 22:43 UTC
- 編集日時: 2020 年 12 月 18 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonFSxConsoleFullAccess

説明： Amazon FSx へのフルアクセスと、経由での関連 AWS サービスへのアクセスを提供します
AWS Management Console。

AmazonFSxConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:36 UTC
- 編集日時: 2024 年 1 月 10 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonFSxConsoleReadOnlyAccess

説明： Amazon FSx への読み取り専用アクセスと、経由での関連 AWS サービスへのアクセスを提供します AWS Management Console。

AmazonFSxConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 11 月 28 日 16:35 UTC
- 編集日時: 2024 年 1 月 10 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonFSxFullAccess

説明： Amazon FSx へのフルアクセスと、関連 AWS サービスへのアクセスを提供します。

AmazonFSxFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:34 UTC
- 編集日時: 2024 年 1 月 10 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonFSxReadOnlyAccess

説明： Amazon FSx への読み取り専用アクセスを提供します。

AmazonFSxReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonFSxReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 16:33 UTC
- 編集日時: 2018 年 11 月 28 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonFSxServiceRolePolicy

説明： Amazon FSx がユーザーに代わって AWS リソースを管理することを許可する

AmazonFSxServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 28 日 10:38 UTC
- 編集日時: 2024 年 1 月 10 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGlacierFullAccess

説明： 経由で Amazon Glacier へのフルアクセスを提供します AWS Management Console。

AmazonGlacierFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGlacierFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGlacierReadOnlyAccess

説明： 経由で Amazon Glacier への読み取り専用アクセスを提供します AWS Management Console。

AmazonGlacierReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGlacierReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 5 月 5 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGrafanaAthenaAccess

説明：このポリシーは、Amazon Grafana の Amazon Athena プラグインから s3 へのクエリと結果の書き込みを有効にするために必要な依存関係と Amazon Athena へのアクセスを許可します。

AmazonGrafanaAthenaAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaAthenaAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 22 日 17:11 UTC
- 編集日時: 2021 年 11 月 22 日 17:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonGrafanaCloudWatchAccess

説明： このポリシーは、Amazon へのアクセス CloudWatch と、Amazon Managed Grafana 内のデータソース CloudWatch として を使用するために必要な依存関係を付与します。

AmazonGrafanaCloudWatchAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaCloudWatchAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 3 月 24 日 22:41 UTC
- 編集日時: 2023 年 3 月 24 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGrafanaRedshiftAccess

説明：このポリシーは、Amazon Redshift へのスコープ付きアクセスと、Amazon Grafana で Amazon Redshift プラグインを使用するために必要な依存関係を付与します。

AmazonGrafanaRedshiftAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGrafanaRedshiftAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 26 日 23:15 UTC
- 編集日時: 2021 年 11 月 26 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGrafanaServiceLinkedRolePolicy

説明： Amazon Grafana が管理または使用する AWS リソースへのアクセスを提供します。

AmazonGrafanaServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 11 月 8 日 23:10 UTC
- 編集日時: 2022 年 11 月 8 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGuardDutyFullAccess

説明： Amazon を使用するためのフルアクセスを提供します GuardDuty。

AmazonGuardDutyFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGuardDutyFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 22:31 UTC
- 編集日時: 2024 年 6 月 10 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ],
}
```



```
{
  "Sid" : "ActionsForOrganizationsSid1",
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "IamGetRoleSid1",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
},
{
  "Sid" : "AllowPassRoleToMalwareProtectionPlan",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

説明： GuardDuty マルウェア保護は、 という名前のサービスにリンクされたロール (SLR) を使用します `AWSServiceRoleForAmazonGuardDutyMalwareProtection`。このサービスにリンクされたロールにより、 GuardDuty マルウェア保護はエージェントレススキャンを実行してマルウェアを検出できます。これにより GuardDuty、 アカウントでスナップショットを作成し、そのスナップショットを GuardDuty サービスアカウントと共有してマルウェアをスキャンできます。これらの共有スナップショットを評価し、取得した EC2 インスタンスメタデータを GuardDuty Malware Protection の検出結果に含めます。 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` サービスにリンクされたロールは、 `malware-protection.guardduty.amazonaws.com` サービスを信頼してロールを引き受けます。

AmazonGuardDutyMalwareProtectionServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 19 日 19:06 UTC
- 編集日時: 2024 年 1 月 25 日 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid" : "CreateTagsPermission",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:*/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateSnapshot"
      }
    }
  },
  {
    "Sid" : "AddTagsToSnapshotPermission",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/GuardDutyScanId" : "*"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "GuardDutyExcluded",
          "GuardDutyFindingDetected"
        ]
      }
    }
  },
  {
    "Sid" : "DeleteAndShareSnapshotPermission",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot",
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/GuardDutyScanId" : "*"
      },
      "Null" : {
```

```
        "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
}
},
{
  "Sid" : "PreventPublicAccessToSnapshotPermission",
  "Effect" : "Deny",
  "Action" : [
    "ec2:ModifySnapshotAttribute"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:Add/group" : "all"
    }
  }
},
{
  "Sid" : "CreateGrantPermission",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    },
    "StringLike" : {
      "kms:EncryptionContext:aws:ebs:id" : "snap-*"
    },
    "ForAllValues:StringEquals" : {
      "kms:GrantOperations" : [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
}
```

```
  },
  {
    "Sid" : "ShareSnapshotKMSPermission",
    "Effect" : "Allow",
    "Action" : [
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource" : "arn:aws:kms:*:*:key/*",
    "Condition" : {
      "StringLike" : {
        "kms:ViaService" : "ec2.*.amazonaws.com"
      },
      "Null" : {
        "aws:ResourceTag/GuardDutyExcluded" : "true"
      }
    }
  }
},
{
  "Sid" : "DescribeKeyPermission",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "arn:aws:kms:*:*:key/*"
},
{
  "Sid" : "GuardDutyLogGroupPermission",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs:CreateLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
},
{
  "Sid" : "GuardDutyLogStreamPermission",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
},
```

```
{
  "Sid" : "EBSDirectAPIPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ebs:GetSnapshotBlock",
    "ebs:ListSnapshotBlocks"
  ],
  "Resource" : "arn:aws:ec2:*:*:snapshot/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/GuardDutyScanId" : "*"
    },
    "Null" : {
      "aws:ResourceTag/GuardDutyExcluded" : "true"
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGuardDutyReadOnlyAccess

説明： Amazon GuardDuty リソースへの読み取り専用アクセスを提供します

AmazonGuardDutyReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonGuardDutyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 22:29 UTC
- 編集日時: 2023 年 11 月 16 日 23:07 UTC

- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonGuardDutyServiceRolePolicy

説明： Amazon Guard Duty が使用または管理する AWS リソースへのアクセスを有効にする

AmazonGuardDutyServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 28 日 20:12 UTC
- 編集日時: 2024 年 3 月 27 日 00:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
    }
  },
  {
    "Sid" : "GuardDutyCreateVpcEndpointPolicy",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "GuardDutyManaged"
      },
      "StringLike" : {
        "ec2:VpceServiceName" : [
          "com.amazonaws.*.guardduty-data",
          "com.amazonaws.*.guardduty-data-fips"
        ]
      }
    }
  },
  {
    "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVpcEndpoint",
      "ec2:DeleteVpcEndpoints"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/GuardDutyManaged" : false
      }
    }
  },
  {
    "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVpcEndpoint",
      "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : [
```

```
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:subnet/*"
  ]
},
{
  "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutySecurityGroupManagementPolicy",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2>DeleteSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/GuardDutyManaged" : false
    }
  }
},
{
  "Sid" : "GuardDutyCreateSecurityGroupPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/GuardDutyManaged" : "*"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateSecurityGroup"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutyCreateEksAddonPolicy",
  "Effect" : "Allow",
  "Action" : "eks:CreateAddon",
  "Resource" : "arn:aws:eks:*:*:cluster/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutyEksAddonManagementPolicy",
  "Effect" : "Allow",
  "Action" : [
    "eks>DeleteAddon",
    "eks:UpdateAddon",
    "eks:DescribeAddon"
  ],
  "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
},
```

```
{
  "Sid" : "GuardDutyEksClusterTagResourcePolicy",
  "Effect" : "Allow",
  "Action" : "eks:TagResource",
  "Resource" : "arn:aws:eks:*:*:cluster/*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : "GuardDutyManaged"
    }
  }
},
{
  "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
  "Effect" : "Allow",
  "Action" : "ecs:PutAccountSettingDefault",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:account-setting" : [
        "guardDutyActivate"
      ]
    }
  }
},
{
  "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeAssociation",
    "ssm>DeleteAssociation",
    "ssm:UpdateAssociation",
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce"
  ],
  "Resource" : "arn:aws:ssm:*:*:association/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/GuardDutyManaged" : "true"
    }
  }
},
{
  "Sid" : "SsmAddTagsToResourcePermission",
  "Effect" : "Allow",
```

```
"Action" : [
  "ssm:AddTagsToResource"
],
"Resource" : "arn:aws:ssm:*:*:association/*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "GuardDutyManaged"
    ]
  },
  "StringEquals" : {
    "aws:ResourceTag/GuardDutyManaged" : "true"
  }
}
},
{
  "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
  "Effect" : "Allow",
  "Action" : [
    "ssm:CreateAssociation",
    "ssm:UpdateAssociation"
  ],
  "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
},
{
  "Sid" : "SsmSendCommandPermission",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
  ]
},
{
  "Sid" : "SsmGetCommandStatus",
  "Effect" : "Allow",
  "Action" : "ssm:GetCommandInvocation",
  "Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonHealthLakeFullAccess

説明： Amazon HealthLake サービスへのフルアクセスを提供します。

AmazonHealthLakeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHealthLakeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 01:07 UTC
- 編集日時: 2021 年 2 月 17 日 01:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHealthLakeReadOnlyAccess

説明： Amazon HealthLake サービスへの読み取り専用アクセスを提供します。

AmazonHealthLakeReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHealthLakeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 02:43 UTC
- 編集日時: 2021 年 2 月 17 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeFullAccess

説明： AWS Management Console および SDK 経由で Honeycode へのフルアクセスを提供します。

AmazonHoneycodeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeReadOnlyAccess

説明： AWS Management Console および SDK 経由で Honeycode への読み取り専用アクセスを提供します。

AmazonHoneycodeReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeServiceRolePolicy

説明： Amazon Honeycode がリソースにアクセスするために必要なサービスにリンクされたロール。

AmazonHoneycodeServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:03 UTC
- 編集日時: 2020 年 11 月 18 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeTeamAssociationFullAccess

説明： AWS Management Console および SDK 経由で Honeycode Team Association へのフルアクセスを提供します。

AmazonHoneycodeTeamAssociationFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeTeamAssociationFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Statement" : [
  {
    "Action" : [
      "honeycode:ListTeamAssociations",
      "honeycode:ApproveTeamAssociation",
      "honeycode:RejectTeamAssociation"
    ],
    "Resource" : "*",
    "Effect" : "Allow"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

説明： AWS Management Console および SDK 経由で Honeycode Team Association への読み取り専用アクセスを提供します。

AmazonHoneycodeTeamAssociationReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeTeamAssociationReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:27 UTC
- 編集日時: 2020 年 6 月 24 日 20:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeWorkbookFullAccess

説明 : AWS Management Console および SDK 経由で Honeycode Workbook へのフルアクセスを提供します。

AmazonHoneycodeWorkbookFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeWorkbookFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonHoneycodeWorkbookReadOnlyAccess

説明： AWS Management Console および SDK 経由で Honeycode Workbook への読み取り専用アクセスを提供します。

AmazonHoneycodeWorkbookReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonHoneycodeWorkbookReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 20:28 UTC
- 編集日時: 2020 年 12 月 1 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspector2AgentlessServiceRolePolicy

説明： エージェントレスセキュリティ評価を実行する AWS のサービス ために必要な へのアクセス権を Amazon Inspector に付与します

AmazonInspector2AgentlessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 20 日 15:18 UTC
- 編集日時: 2023 年 11 月 20 日 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspector2FullAccess

説明： Amazon Inspector へのフルアクセスと、組織などの他の関連サービスへのアクセスを提供します。

AmazonInspector2FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 19:10 UTC
- 編集日時: 2024 年 4 月 25 日 13:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspector2ManagedCisPolicy

説明：これは、CIS スキャンのためにインスペクターサービスと通信するために顧客がロールにアタッチする必要がある マネージドポリシーです。

AmazonInspector2ManagedCisPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspector2ManagedCisPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 1 月 24 日 16:31 UTC
- 編集日時: 2024 年 1 月 24 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspector2ReadOnlyAccess

説明： Amazon Inspector2 サービスおよび関連するサポートサービスへの読み取り専用アクセスを提供します

AmazonInspector2ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonInspector2ReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 1 月 21 日 14:45 UTC
- 編集日時: 2023 年 9 月 22 日 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspector2ServiceRolePolicy

説明：セキュリティ評価の実行 AWS のサービスに必要な へのアクセス権を Amazon Inspector に付与します

AmazonInspector2ServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 16 日 20:27 UTC
- 編集日時: 2024 年 1 月 22 日 14:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonInspectorFullAccess

説明： Amazon Inspector へのフルアクセスを提供します。

AmazonInspectorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspectorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2017 年 12 月 21 日 14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspectorReadOnlyAccess

説明： Amazon Inspector への読み取り専用アクセスを提供します。

AmazonInspectorReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonInspectorReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 17:08 UTC
- 編集日時: 2019 年 10 月 1 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonInspectorServiceRolePolicy

説明：セキュリティ評価の実行 AWS のサービスに必要な へのアクセス権を Amazon Inspector に付与します

AmazonInspectorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 21 日 15:48 UTC
- 編集日時: 2020 年 9 月 11 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKendraFullAccess

説明： 経由で Amazon Kendra へのフルアクセスを提供します AWS Management Console。

AmazonKendraFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKendraFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:15 UTC
- 編集日時: 2019 年 12 月 3 日 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonKendraReadOnlyAccess

説明： 経由で Amazon Kendra への読み取り専用アクセスを提供します AWS Management Console。

AmazonKendraReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKendraReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2019 年 12 月 3 日 16:13 UTC
- 編集日時: 2021 年 5 月 27 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKeyspacesFullAccess

説明： Amazon Keyspaces へのフルアクセスを提供する

AmazonKeyspacesFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 23 日 17:06 UTC
- 編集日時: 2023 年 10 月 3 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKeyspacesReadOnlyAccess

説明： Amazon Keyspaces への読み取り専用アクセスを提供する

AmazonKeyspacesReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 4 月 23 日 17:07 UTC
- 編集日時: 2022 年 7 月 7 日 14:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKeyspacesReadOnlyAccess_v2

説明： Amazon Keyspaces および関連 AWS サービスへの読み取り専用アクセスを提供します。

AmazonKeyspacesReadOnlyAccess_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKeyspacesReadOnlyAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 12 日 17:01 UTC
- 編集日時: 2023 年 9 月 12 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisAnalyticsFullAccess

説明： 経由で Amazon Kinesis Analytics へのフルアクセスを提供します AWS Management Console。

AmazonKinesisAnalyticsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 9 月 21 日 19:01 UTC
- 編集日時: 2016 年 9 月 21 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "kinesis:CreateStream",
        "kinesis>DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "logs:GetLogEvents",
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
}
]
```

}

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisAnalyticsReadOnly

説明： 経由で Amazon Kinesis Analytics への読み取り専用アクセスを提供します AWS Management Console。

AmazonKinesisAnalyticsReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisAnalyticsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 9 月 21 日 18:16 UTC
- 編集日時: 2016 年 9 月 21 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisFirehoseFullAccess

説明：すべての Amazon Kinesis Firehose 配信ストリームへのフルアクセスを提供します。

AmazonKinesisFirehoseFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisFirehoseFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 18:45 UTC
- 編集日時: 2015 年 10 月 7 日 18:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisFirehoseReadOnlyAccess

説明：すべての Amazon Kinesis Firehose 配信ストリームへの読み取り専用アクセスを提供します。

AmazonKinesisFirehoseReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisFirehoseReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 7 日 18:43 UTC
- 編集日時: 2015 年 10 月 7 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisFullAccess

説明： 経由ですべてのストリームへのフルアクセスを提供します AWS Management Console。

AmazonKinesisFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisReadOnlyAccess

説明： 経由ですべてのストリームへの読み取り専用アクセスを提供します AWS Management Console。

AmazonKinesisReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisVideoStreamsFullAccess

説明： 経由で Amazon Kinesis Video Streams へのフルアクセスを提供します AWS Management Console。

AmazonKinesisVideoStreamsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisVideoStreamsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2017 年 12 月 1 日 23:27 UTC
- 編集日時: 2017 年 12 月 1 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonKinesisVideoStreamsReadOnlyAccess

説明： 経由で AWS Kinesis Video Streams への読み取り専用アクセスを提供します AWS Management Console。

AmazonKinesisVideoStreamsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonKinesisVideoStreamsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 1 日 23:14 UTC
- 編集日時: 2017 年 12 月 1 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLaunchWizard_Fullaccess

説明： AWS 起動ウィザードおよびその他の必要なサービスへのフルアクセス。

AmazonLaunchWizard_Fullaccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizard_Fullaccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 6 日 17:47 UTC
- 編集日時: 2023 年 2 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLaunchWizardFullAccessV2

説明： AWS 起動ウィザードおよびその他の必要なサービスへのフルアクセス。

AmazonLaunchWizardFullAccessV2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLaunchWizardFullAccessV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 1 日 17:14 UTC
- 編集日時: 2023 年 9 月 1 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLexChannelsAccess

説明：このポリシーでは、お客様はチャンネルから Lex ランタイムを呼び出すことができます。

AmazonLexChannelsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:12 UTC
- 編集日時: 2021 年 1 月 13 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLexFullAccess

説明： 経由で Amazon Lex へのフルアクセスを提供します AWS Management Console。また、Lex サービスにリンクされたロールを作成し、限定された Lambda 関数セットを呼び出すための Lex アクセス許可を付与するためのアクセスも提供します。

AmazonLexFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:20 UTC
- 編集日時: 2024 年 4 月 16 日 20:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
    },
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AmazonLexFullAccessStatement2",
    "Effect" : "Allow",
    "Action" : [
      "lambda:AddPermission",
      "lambda:RemovePermission"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
    "Condition" : {
      "StringEquals" : {
        "lambda:Principal" : "lex.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement3",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole"
    ],
    "Resource" : [
      "arn:aws:iam:*:*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
      "arn:aws:iam:*:*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
      "arn:aws:iam:*:*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
      "arn:aws:iam:*:*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
      "arn:aws:iam:*:*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ]
  },
  {
    "Sid" : "AmazonLexFullAccessStatement4",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
```

```
    "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "lex.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement5",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "channels.lex.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement6",
  "Effect" : "Allow",
  "Action" : [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "lexv2.amazonaws.com"
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement7",
  "Effect" : "Allow",
```

```
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement8",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement9",
    "Effect" : "Allow",
    "Action" : [
      "iam>DeleteServiceLinkedRole",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
      "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
      "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",

```

```
    "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
    "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
  ]
},
{
  "Sid" : "AmazonLexFullAccessStatement10",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "lex.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement11",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "lexv2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AmazonLexFullAccessStatement12",
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "channels.lexv2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonLexFullAccessStatement13",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lexv2.amazonaws.com"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLexReadOnly

説明： Amazon Lex への読み取り専用アクセスを提供します。

AmazonLexReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:13 UTC
- 編集日時: 2024 年 5 月 13 日 16:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
```

```
"lex:GetBots",
"lex:GetBotChannelAssociation",
"lex:GetBotChannelAssociations",
"lex:GetBotVersions",
"lex:GetBuiltinIntent",
"lex:GetBuiltinIntents",
"lex:GetBuiltinSlotTypes",
"lex:GetIntent",
"lex:GetIntents",
"lex:GetIntentVersions",
"lex:GetSlotType",
"lex:GetSlotTypes",
"lex:GetSlotTypeVersions",
"lex:GetUtterancesView",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotChannel",
"lex:DescribeBotLocale",
"lex:DescribeBotRecommendation",
"lex:DescribeBotReplica",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:ListBots",
"lex:ListBotLocales",
"lex:ListBotAliases",
"lex:ListBotAliasReplicas",
"lex:ListBotChannels",
"lex:ListBotRecommendations",
"lex:ListBotReplicas",
"lex:ListBotVersions",
"lex:ListBotVersionReplicas",
"lex:ListBuiltinIntents",
"lex:ListBuiltinSlotTypes",
"lex:ListExports",
"lex:ListImports",
"lex:ListIntents",
"lex:ListRecommendedIntents",
"lex:ListSlots",
"lex:ListSlotTypes",
```

```
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLexReplicationPolicy

説明： Amazon Lex がユーザーに代わってリージョン間で Lex リソースをレプリケートできるようにします。

AmazonLexReplicationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 1 月 31 日 23:29 UTC
- 編集日時: 2024 年 3 月 8 日 17:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLexRunBotsOnly

説明 : Amazon Lex 会話 APIs。

AmazonLexRunBotsOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLexRunBotsOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 11 日 23:06 UTC
- 編集日時: 2021 年 8 月 18 日 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLexV2BotPolicy

説明： Lex V2 ボットがユーザーに代わって他の AWS サービスを呼び出すためのアクセスを提供します。

AmazonLexV2BotPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 13 日 20:10 UTC
- 編集日時: 2021 年 1 月 13 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutEquipmentFullAccess

説明： Amazon Lookout for Equipment オペレーションへのフルアクセスを提供します

AmazonLookoutEquipmentFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutEquipmentFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 8 日 15:52 UTC
- 編集日時: 2021 年 11 月 24 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutEquipmentReadOnlyAccess

説明： Amazon Lookout for Equipments への読み取り専用アクセスを提供します

AmazonLookoutEquipmentReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutEquipmentReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 5 日 16:47 UTC
- 編集日時: 2022 年 11 月 10 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutMetricsFullAccess

説明： Amazon Lookout for Metrics のすべてのアクションへのアクセスを許可します

AmazonLookoutMetricsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutMetricsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2021 年 5 月 7 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutMetricsReadOnlyAccess

説明： Amazon Lookout for Metrics のすべての読み取り専用アクションへのアクセスを許可します

AmazonLookoutMetricsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutMetricsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 7 日 00:43 UTC
- 編集日時: 2022 年 1 月 4 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutVisionConsoleFullAccess

説明： Amazon Lookout for Vision へのフルアクセスと、必要なサービスおよびコンソールの依存関係へのスコープ付きアクセスを提供します。

AmazonLookoutVisionConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:37 UTC
- 編集日時: 2021 年 5 月 11 日 19:37 UTC

- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutVisionConsoleReadOnlyAccess

説明： Amazon Lookout for Vision への読み取り専用アクセスと、必要なサービスおよびコンソールの依存関係へのスコープ付きアクセスを提供します。

AmazonLookoutVisionConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 5 月 11 日 19:32 UTC
- 編集日時: 2021 年 12 月 9 日 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutVisionFullAccess

説明： Amazon Lookout for Vision へのフルアクセスと、必要な依存関係へのスコープ付きアクセスを提供します。

AmazonLookoutVisionFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:24 UTC
- 編集日時: 2021 年 5 月 11 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonLookoutVisionReadOnlyAccess

説明： Amazon Lookout for Vision への読み取り専用アクセスと、必要な依存関係へのスコープ付きアクセスを提供します。

AmazonLookoutVisionReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonLookoutVisionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 11 日 19:11 UTC
- 編集日時: 2021 年 12 月 9 日 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningBatchPredictionsAccess

説明： Amazon Machine Learning バッチ予測をリクエストするアクセス許可をユーザーに付与します。

AmazonMachineLearningBatchPredictionsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningBatchPredictionsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:12 UTC
- 編集日時: 2015 年 4 月 9 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningCreateOnlyAccess

説明： 予測以外の Amazon Machine Learning リソースの作成アクセスを提供します。

AmazonMachineLearningCreateOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningCreateOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:18 UTC
- 編集日時: 2016 年 6 月 29 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningFullAccess

説明： Amazon Machine Learning リソースへのフルアクセスを提供します。

AmazonMachineLearningFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:25 UTC
- 編集日時: 2015 年 4 月 9 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

説明： Amazon Machine Learning モデルのリアルタイムエンドポイントを作成および削除するアクセス許可をユーザーに付与します。

AmazonMachineLearningManageRealTimeEndpointOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonMachineLearningManageRealTimeEndpointOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:32 UTC
- 編集日時: 2015 年 4 月 9 日 17:32 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningReadOnlyAccess

説明: Amazon Machine Learning リソースへの読み取り専用アクセスを提供します。

AmazonMachineLearningReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonMachineLearningReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:40 UTC
- 編集日時: 2015 年 4 月 9 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

説明： Amazon Machine Learning のリアルタイム予測をリクエストするアクセス許可をユーザーに付与します。

AmazonMachineLearningRealTimePredictionOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonMachineLearningRealTimePredictionOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 17:44 UTC
- 編集日時: 2015 年 4 月 9 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

説明 : Machine Learning が Redshift データソースの Redshift クラスターと S3 ステージング場所を設定して使用できるようにします。

AmazonMachineLearningRoleforRedshiftDataSourceV3 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMachineLearningRoleforRedshiftDataSourceV3 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 24 日 18:00 UTC
- 編集日時: 2020 年 6 月 24 日 18:00 UTC

- ARN: arn:aws:iam::aws:policy/service-role/
AmazonMachineLearningRoleforRedshiftDataSourceV3

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMacieFullAccess

説明： Amazon Macie へのフルアクセスを提供します。

AmazonMacieFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 14:54 UTC
- 編集日時: 2022 年 7 月 1 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMacieHandshakeRole

説明： Amazon Macie のサービスにリンクされたロールを作成するアクセス許可を付与します。

AmazonMacieHandshakeRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieHandshakeRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 28 日 15:46 UTC
- 編集日時: 2018 年 6 月 28 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMacieReadOnlyAccess

説明： Amazon Macie への読み取り専用アクセスを提供します。

AmazonMacieReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 15 日 21:50 UTC
- 編集日時: 2023 年 6 月 15 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMacieServiceRole

説明：データ分析を有効にするために、アカウントのリソース依存関係への読み取り専用アクセスを Macie に付与します。

AmazonMacieServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMacieServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:53 UTC
- 編集日時: 2017 年 8 月 14 日 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMacieServiceRolePolicy

説明： Amazon Macie のサービスにリンクされたロール

AmazonMacieServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 19 日 22:17 UTC
- 編集日時: 2022 年 5 月 19 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
```

```
    "s3:ListAllMyBuckets",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListBucket",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectTagging"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
  ]
}
]
```


詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonManagedBlockchainConsoleFullAccess

説明： 経由で Amazon Managed Blockchain へのフルアクセスを提供します AWS Management Console

AmazonManagedBlockchainConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 29 日 21:23 UTC
- 編集日時: 2019 年 4 月 29 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "managedblockchain:*",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:CreateVpcEndpoint",
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonManagedBlockchainFullAccess

説明： Amazon Managed Blockchain へのフルアクセスを提供します。

AmazonManagedBlockchainFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 29 日 21:39 UTC

- 編集日時: 2019 年 4 月 29 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonManagedBlockchainReadOnlyAccess

説明: Amazon Managed Blockchain への読み取り専用アクセスを提供します。

AmazonManagedBlockchainReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonManagedBlockchainReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 30 日 18:17 UTC
- 編集日時: 2019 年 4 月 30 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonManagedBlockchainServiceRolePolicy

説明： Amazon Managed Blockchain が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする

AmazonManagedBlockchainServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 17 日 19:51 UTC
- 編集日時: 2020 年 1 月 17 日 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMCSFullAccess

説明 : Amazon Managed Apache Cassandra サービスへのフルアクセスを提供する

AmazonMCSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 13:45 UTC
- 編集日時: 2020 年 4 月 17 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMCSReadOnlyAccess

説明 : Amazon Managed Apache Cassandra Service への読み取り専用アクセスを提供する

AmazonMCSReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMCSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 13:46 UTC
- 編集日時: 2020 年 4 月 17 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMechanicalTurkFullAccess

説明： Amazon Mechanical Turk のすべての APIs へのフルアクセスを提供します。

AmazonMechanicalTurkFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMechanicalTurkFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC
- 編集日時: 2015 年 12 月 11 日 19:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMechanicalTurkReadOnly

説明： Amazon Mechanical Turk の読み取り専用 APIs へのアクセスを提供します。

AmazonMechanicalTurkReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMechanicalTurkReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 12 月 11 日 19:08 UTC
- 編集日時: 2019 年 9 月 25 日 21:06 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMemoryDBFullAccess

説明： 経由で Amazon MemoryDB へのフルアクセスを提供します AWS Management Console。

AmazonMemoryDBFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMemoryDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 8 日 19:24 UTC
- 編集日時: 2021 年 10 月 8 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMemoryDBReadOnlyAccess

説明： 経由で Amazon MemoryDB への読み取り専用アクセスを提供します AWS Management Console。

AmazonMemoryDBReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMemoryDBReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 8 日 19:27 UTC
- 編集日時: 2021 年 10 月 8 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMobileAnalyticsFinancialReportAccess

説明：すべてのアプリケーションリソースの財務データを含むすべてのレポートへの読み取り専用アクセスを提供します。

AmazonMobileAnalyticsFinancialReportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFinancialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMobileAnalyticsFullAccess

説明: すべてのアプリケーションリソースへのフルアクセスを提供します。

AmazonMobileAnalyticsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMobileAnalyticsNon-financialReportAccess

説明：すべてのアプリケーションリソースの非財務レポートへの読み取り専用アクセスを提供します。

AmazonMobileAnalyticsNon-financialReportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsNon-financialReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Effect" : "Allow",
  "Action" : "mobileanalytics:GetReports",
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMobileAnalyticsWriteOnlyAccess

説明：すべてのアプリケーションリソースのイベントデータを配置するための書き込み専用アクセスを提供します。(SDK 統合に推奨)

AmazonMobileAnalyticsWriteOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMobileAnalyticsWriteOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMonitronFullAccess

説明： Amazon Monitron を管理するためのフルアクセスを提供します

AmazonMonitronFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMonitronFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 2 日 22:40 UTC
- 編集日時: 2022 年 6 月 8 日 16:27 UTC

- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMQApiFullAccess

説明： API/SDK 経由で AmazonMQ へのフルアクセスを提供します。

AmazonMQApiFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQApiFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC
- 編集日時: 2020 年 11 月 4 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMQApiReadOnlyAccess

説明： API/SDK 経由で AmazonMQ への読み取り専用アクセスを提供します。

AmazonMQApiReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQApiReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 18 日 20:31 UTC
- 編集日時: 2018 年 12 月 18 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Action" : [
    "mq:Describe*",
    "mq:List*",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMQFullAccess

説明： 経由で AmazonMQ へのフルアクセスを提供します AWS Management Console。

AmazonMQFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 15:28 UTC
- 編集日時: 2020 年 11 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMQReadOnlyAccess

説明： 経由で AmazonMQ への読み取り専用アクセスを提供します AWS Management Console。

AmazonMQReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMQReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 28 日 15:30 UTC
- 編集日時: 2017 年 11 月 28 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMQServiceRolePolicy

説明: AWS Amazon MQ のサービスリンクロールポリシー

AmazonMQServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 4 日 16:07 UTC
- 編集日時: 2020 年 11 月 4 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMSKConnectReadOnlyAccess

説明： Amazon MSK Connect への読み取り専用アクセスを提供する

AmazonMSKConnectReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 20 日 10:18 UTC
- 編集日時: 2021 年 10 月 18 日 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMSKFullAccess

説明： Amazon MSK へのフルアクセスと、その依存関係に必要なその他のアクセス許可を提供します。

AmazonMSKFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 14 日 22:07 UTC
- 編集日時: 2023 年 10 月 18 日 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonMSKReadOnlyAccess

説明： Amazon MSK への読み取り専用アクセスを提供する

AmazonMSKReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonMSKReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 14 日 22:28 UTC
- 編集日時: 2019 年 1 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonMWAAServiceRolePolicy

説明: Amazon Managed Workflows for Apache Airflow で使用されるサービスリンクロール。

AmazonMWAAServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 24 日 14:13 UTC
- 編集日時: 2022 年 11 月 17 日 00:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonNimbleStudio-LaunchProfileWorker

説明：このポリシーは、Nimble Studio Launch Profile ワーカーが必要とするリソースへのアクセスを許可します。Nimble Studio Builder で作成された EC2 インスタンスにこのポリシーをアタッチします。

AmazonNimbleStudio-LaunchProfileWorker は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-LaunchProfileWorker をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2021 年 4 月 28 日 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonNimbleStudio-StudioAdmin

説明：このポリシーは、スタジオ管理者に関連付けられた Amazon Nimble Studio リソースおよび他のサービスの関連するスタジオリソースへのアクセスを許可します。このポリシーをスタジオに関連する管理者ロールにアタッチしてください。

AmazonNimbleStudio-StudioAdmin は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:47 UTC
- 編集日時: 2023 年 9 月 22 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonNimbleStudio-StudioUser

説明：このポリシーは、スタジオユーザーに関連付けられた Amazon Nimble Studio リソースおよび他のサービスの関連するスタジオリソースへのアクセスを許可します。このポリシーをスタジオに関連付けられているユーザーロールにアタッチしてください。

AmazonNimbleStudio-StudioUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonNimbleStudio-StudioUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 28 日 04:48 UTC
- 編集日時: 2023 年 9 月 22 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOmicsFullAccess

説明： Amazon Omics およびその他の必要な へのフルアクセスを提供します AWS のサービス。このポリシーにより、ユーザーは RAM 共有の招待を表示して承諾し、ユーザーの AWS アカウント以外のリソースにアクセスすることができます。

AmazonOmicsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOmicsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 2 月 24 日 00:59 UTC
- 編集日時: 2023 年 2 月 24 日 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOmicsReadOnlyAccess

説明： Amazon Omics への読み取り専用アクセスを提供する

AmazonOmicsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOmicsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 29 日 04:17 UTC
- 編集日時: 2022 年 11 月 29 日 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOneEnterpriseFullAccess

説明：このポリシーは、すべての Amazon One Enterprise リソースとオペレーションへのアクセスを許可する管理アクセス許可を付与します。

AmazonOneEnterpriseFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 04:58 UTC
- 編集日時: 2023 年 11 月 28 日 04:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOneEnterpriseInstallerAccess

説明: このポリシーは、デバイスのインストールとアクティベーションを許可する制限付き読み取りおよび書き込みアクセス許可を付与します。

AmazonOneEnterpriseInstallerAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseInstallerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 05:00 UTC
- 編集日時: 2023 年 11 月 28 日 05:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
```

```
        "one:ListDeviceInstances",
        "one:ListSites"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOneEnterpriseReadOnlyAccess

説明：このポリシーは、すべての Amazon One Enterprise リソースとオペレーションに読み取り専用アクセス許可を付与します。

AmazonOneEnterpriseReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOneEnterpriseReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 04:59 UTC
- 編集日時: 2023 年 11 月 28 日 04:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchDashboardsServiceRolePolicy

説明 : Amazon OpenSearch Dashboards Service にアクセスして、 CloudWatch ユーザーに代わってなどの他の AWS サービスにアクセスする

AmazonOpenSearchDashboardsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 12 月 22 日 19:38 UTC
- 編集日時: 2023 年 12 月 22 日 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchDirectQueryGlueCreateAccess

説明： OpenSearch DirectQuery サービスがユーザーに代わってリソースを作成するための AWS Glue APIs にアクセスできるようにします。

AmazonOpenSearchDirectQueryGlueCreateAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchDirectQueryGlueCreateAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 5 月 6 日 12:24 UTC
- 編集日時: 2024 年 5 月 6 日 12:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
    "Effect" : "Allow",
    "Action" : [
      "glue:CreateDatabase",
      "glue:CreatePartition",
      "glue:CreateTable",
      "glue:BatchCreatePartition"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchIngestionFullAccess

説明： Amazon OpenSearch Ingestion がユーザーに代わって他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchIngestionFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 26 日 18:11 UTC

- 編集日時: 2023 年 4 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchIngestionReadOnlyAccess

説明 : Amazon Ingestion Service OpenSearch への読み取り専用アクセスを提供します

AmazonOpenSearchIngestionReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchIngestionReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 26 日 18:09 UTC
- 編集日時: 2023 年 4 月 26 日 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchIngestionServiceRolePolicy

説明： Amazon OpenSearch Ingestion Service がユーザーに代わって他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchIngestionServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 18 日 16:49 UTC
- 編集日時: 2022 年 11 月 18 日 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchServerlessServiceRolePolicy

説明： Amazon OpenSearch Serverless がユーザーに代わって CloudWatch APIsなどの他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchServerlessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 24 日 19:50 UTC
- 編集日時: 2022 年 11 月 24 日 19:50 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchServiceCognitoAccess

説明 : Amazon Cognito 設定サービスへのアクセスを提供します。

AmazonOpenSearchServiceCognitoAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceCognitoAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 2 日 06:31 UTC
- 編集日時: 2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchServiceFullAccess

説明 : Amazon OpenSearch Service 設定サービスへのフルアクセスを提供します。

AmazonOpenSearchServiceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 8 日 05:33 UTC
- 編集日時: 2021 年 9 月 8 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchServiceReadOnlyAccess

説明： Amazon OpenSearch Service 設定サービスへの読み取り専用アクセスを提供します。

AmazonOpenSearchServiceReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonOpenSearchServiceReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 8 日 05:38 UTC
- 編集日時: 2021 年 9 月 8 日 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Action" : [
      "es:Describe*",
      "es:List*",
      "es:Get*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonOpenSearchServiceRolePolicy

説明： Amazon OpenSearch Service がユーザーに代わって EC2 Networking APIsなどの他の AWS サービスにアクセスできるようにします。

AmazonOpenSearchServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 26 日 09:27 UTC
- 編集日時: 2023 年 10 月 23 日 07:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonPersonalizeFullAccess

説明：AWS Management Console および SDK 経由で Amazon Personalize へのフルアクセスを提供します。また、関連サービス (S3 など CloudWatch) への選択アクセスも提供します。

AmazonPersonalizeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPersonalizeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 12 月 4 日 22:24 UTC
- 編集日時: 2019 年 5 月 30 日 23:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonPollyFullAccess

説明： Amazon Polly サービスとリソースへのフルアクセスを許可します。

AmazonPollyFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPollyFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2016 年 11 月 30 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonPollyReadOnlyAccess

説明： Amazon Polly リソースへの読み取り専用アクセスを許可します。

AmazonPollyReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPollyReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 18:59 UTC
- 編集日時: 2018 年 7 月 17 日 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
"Action" : [
  "polly:DescribeVoices",
  "polly:GetLexicon",
  "polly:GetSpeechSynthesisTask",
  "polly:ListLexicons",
  "polly:ListSpeechSynthesisTasks",
  "polly:SynthesizeSpeech"
],
"Resource" : [
  "*"
]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonPrometheusConsoleFullAccess

説明: AWS コンソールで AWS Managed Prometheus リソースへのフルアクセスを付与します

AmazonPrometheusConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:11 UTC
- 編集日時: 2022 年 10 月 24 日 22:25 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonPrometheusFullAccess

説明 : AWS Managed Prometheus リソースへのフルアクセスを付与します

AmazonPrometheusFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:10 UTC
- 編集日時 : 2023 年 11 月 26 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonPrometheusQueryAccess

説明 : AWS Managed Prometheus リソースに対してクエリを実行するアクセス許可を付与します

AmazonPrometheusQueryAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusQueryAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 19 日 01:02 UTC
- 編集日時: 2020 年 12 月 19 日 01:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonPrometheusRemoteWriteAccess

説明 : AWS Managed Prometheus ワークスペースへの書き込みのみのアクセスを付与します

AmazonPrometheusRemoteWriteAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonPrometheusRemoteWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 12 月 19 日 01:04 UTC
- 編集日時: 2020 年 12 月 19 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonPrometheusScraperserviceRolePolicy

説明: Amazon Managed Service for Prometheus Collector が管理または使用する AWS リソースへのアクセスを提供します

AmazonPrometheusScrapperServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 26 日 14:19 UTC
- 編集日時: 2024 年 4 月 26 日 20:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapperServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*"
    },
    {
      "Sid" : "NetworkDiscovery",
```



```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribeSubnets",
  "ec2:DescribeSecurityGroups"
],
"Resource" : "*"
},
{
  "Sid" : "ENIManagement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AMPAgentlessScraper"
      ]
    }
  }
},
{
  "Sid" : "TagManagement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkInterface"
    },
    "Null" : {
      "aws:RequestTag/AMPAgentlessScraper" : "false"
    }
  }
},
{
  "Sid" : "ENIUpdating",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "*",
  "Condition" : {
```

```
    "Null" : {
      "ec2:ResourceTag/AMPAgentlessScrapper" : "false"
    }
  },
  {
    "Sid" : "EKSAccess",
    "Effect" : "Allow",
    "Action" : "eks:DescribeCluster",
    "Resource" : "arn:aws:eks:*:*:cluster/*"
  },
  {
    "Sid" : "DeleteEKSAccessEntry",
    "Effect" : "Allow",
    "Action" : "eks:DeleteAccessEntry",
    "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      },
      "ArnLike" : {
        "eks:principalArn" : "arn:aws:iam:*:*:role/aws-service-role/scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*"
      }
    }
  },
  {
    "Sid" : "APSWriting",
    "Effect" : "Allow",
    "Action" : "aps:RemoteWrite",
    "Resource" : "arn:aws:aps:*:*:workspace/*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonQFullAccess

説明 : Amazon Q とのやり取りを有効にするためのフルアクセスを提供します

AmazonQFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 28 日 16:00 UTC
- 編集日時: 2024 年 4 月 29 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowSetTrustedIdentity",
    "Effect" : "Allow",
    "Action" : [
      "sts:SetContext"
    ],
    "Resource" : "arn:aws:sts::*:self"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonQLDBConsoleFullAccess

説明： 経由で Amazon QLDB へのフルアクセスを提供します AWS Management Console。

AmazonQLDBConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:24 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonQLDBFullAccess

説明： サービス API 経由で Amazon QLDB へのフルアクセスを提供します。

AmazonQLDBFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:23 UTC
- 編集日時: 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonQLDBReadOnly

説明： Amazon QLDB への読み取り専用アクセスを提供します。

AmazonQLDBReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonQLDBReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 9 月 5 日 18:19 UTC
- 編集日時: 2021 年 7 月 2 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSBetaServiceRolePolicy

説明： Amazon RDS がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSBetaServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 2 日 19:41 UTC
- 編集日時: 2022 年 12 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSCustomInstanceProfileRolePolicy

説明： Amazon RDS Custom が EC2 インスタンスプロファイルを介してさまざまなオートメーションアクションとデータベース管理タスクを実行できるようにします。

AmazonRDSCustomInstanceProfileRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSCustomInstanceProfileRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 2 月 27 日 17:42 UTC
- 編集日時: 2024 年 2 月 27 日 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSCustomPreviewServiceRolePolicy

説明 : Amazon RDS Custom Preview Service ロールポリシー

AmazonRDSCustomPreviewServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:44 UTC
- 編集日時: 2023 年 9 月 20 日 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSCustomServiceRolePolicy

説明： Amazon RDS Custom がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSCustomServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 8 日 21:39 UTC
- 編集日時: 2024 年 4 月 19 日 15:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
```



```
    "ec2:DisassociateIamInstanceProfile",
    "ec2:AssociateIamInstanceProfile",
    "ec2:ReplaceIamInstanceProfileAssociation",
    "ec2:TerminateInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:RebootInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AllocateAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
```

```
    "ec2:ReleaseAddress"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ecc1scoping3",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssignPrivateIpAddresses"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances1",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:network-interface*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
```

```
        "custom-oracle-rac"
      ]
    }
  },
  {
    "Sid" : "eccRunInstances2",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
      "arn:aws:ec2:*:*:placement-group*"
    ]
  },
  {
    "Sid" : "eccRunInstances3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:snapshot*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac",
          "custom-oracle"
        ]
      }
    }
  },
  {
    "Sid" : "eccModifyInstanceAttribute1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyInstanceAttribute"
    ],
```

```
"Resource" : [
  "arn:aws:ec2:*:*:instance/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/AWSRDSCustom" : [
      "custom-sqlserver"
    ],
    "ec2:Attribute" : "InstanceType"
  }
},
{
  "Sid" : "RequireImsdV2",
  "Effect" : "Deny",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringNotEquals" : {
      "ec2:MetadataHttpTokens" : "required"
    },
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccRunInstances3keyPair1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances",
    "ec2:DeleteKeyPair"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
    ]
  }
}
},
{
  "Sid" : "eccKeyPair2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateKeyPair"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccNetworkInterface1",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : "arn:aws:ec2:*:*:network-interface/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccNetworkInterface2",
  "Effect" : "Allow",
  "Action" : "ec2:CreateNetworkInterface",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
}
```

```
  },
  {
    "Sid" : "eccNetworkInterface3",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteNetworkInterface",
    "Resource" : "arn:aws:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccCreateTag1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccCreateTag2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  }
}
```

```
    ],
    "ec2:CreateAction" : [
      "CreateKeyPair",
      "RunInstances",
      "CreateNetworkInterface",
      "CreateVolume",
      "CreateSnapshot",
      "CreateSnapshots",
      "CopySnapshot",
      "AllocateAddress"
    ]
  }
}
},
{
  "Sid" : "eccVolume1",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccVolume2",
  "Effect" : "Allow",
  "Action" : "ec2:CreateVolume",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
```

```
        "custom-sqlserver",
        "custom-oracle-rac"
    ]
}
},
{
    "Sid" : "eccVolume3",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2>DeleteVolume",
        "ec2:ModifyVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid" : "eccVolume4snapshot1",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVolume",
        "ec2>DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
```



```
"Sid" : "eccSnapshot2",
"Effect" : "Allow",
"Action" : [
  "ec2:CopySnapshot",
  "ec2:CreateSnapshot",
  "ec2:CreateSnapshots"
],
"Resource" : "arn:aws:ec2:*:*:snapshot/*",
"Condition" : {
  "StringLike" : {
    "aws:RequestTag/AWSRDSCustom" : [
      "custom-oracle",
      "custom-sqlserver",
      "custom-oracle-rac"
    ]
  }
},
{
  "Sid" : "eccSnapshot3",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshots",
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eccSnapshot4",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSnapshot",
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
```

```
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-sqlserver"
      ]
    }
  },
  {
    "Sid" : "iam1",
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:GetInstanceProfile",
      "iam:GetRole",
      "iam:ListRolePolicies",
      "iam:GetRolePolicy",
      "iam:ListAttachedRolePolicies",
      "iam:GetPolicy",
      "iam:GetPolicyVersion"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "iam2",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/AWSRDSCustom*",
      "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "cloudtrail1",
    "Effect" : "Allow",
    "Action" : [
      "cloudtrail:GetTrailStatus"
    ],
    "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
  },
}
```

```
{
  "Sid" : "cw1",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:EnableAlarmActions",
    "cloudwatch>DeleteAlarms"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "cw2",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:TagResource"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "cw3",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
},
```

```
{
  "Sid" : "ssm1",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ssm:*:*:document/*"
},
{
  "Sid" : "ssm2",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "ssm3",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetCommandInvocation",
    "ssm:GetConnectionStatus",
    "ssm:DescribeInstanceInformation"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ssm4",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter",
    "ssm:AddTagsToResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "ssm5",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DeleteParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eb1",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule",
    "events:TagResource"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eb2",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:DescribeRule",
    "events:EnableRule",
    "events:ListTargetsByRule",
```

```
    "events:DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/AWSRDSCustom" : [
        "custom-oracle",
        "custom-sqlserver",
        "custom-oracle-rac"
      ]
    }
  }
},
{
  "Sid" : "eb3",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "events:ManagedBy" : [
        "custom.rds.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "eb4",
  "Effect" : "Allow",
  "Action" : [
    "events:PutTargets",
    "events:EnableRule",
    "events:DeleteRule",
    "events:RemoveTargets",
    "events:DisableRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
  "Condition" : {
    "StringLike" : {
      "events:ManagedBy" : [
```

```
        "custom.rds.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "eb5",
    "Effect" : "Allow",
    "Action" : [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
  },
  {
    "Sid" : "secretmanager1",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "secretmanager2",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:TagResource",
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
    "Condition" : {
      "StringLike" : {
```

```
        "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
        ]
    }
},
{
    "Sid" : "sqs1",
    "Effect" : "Allow",
    "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
    ],
    "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/AWSRDSCustom" : [
                "custom-sqlserver"
            ]
        }
    }
},
{
    "Sid" : "sqs2",
    "Effect" : "Allow",
    "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs>DeleteQueue"
    ],
    "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/AWSRDSCustom" : [
                "custom-sqlserver"
            ]
        }
    }
},
{
```



```
    "Sid" : "servicequota1",
    "Effect" : "Allow",
    "Action" : [
        "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSDDataFullAccess

説明 : RDS データ APIs APIs、DB コンソールクエリ管理 APIs を使用して、の Aurora Serverless クラスターで SQL ステートメントを実行するためのフルアクセスを許可します AWS アカウント。

AmazonRDSDDataFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSDDataFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 20 日 21:29 UTC
- 編集日時: 2019 年 11 月 20 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSDDataFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSDirectoryServiceAccess

説明：ドメインに参加している SQL Server DB インスタンスについて、RDS がお客様に代わって Directory Service Managed AD にアクセスできるようにします。

AmazonRDSDirectoryServiceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSDirectoryServiceAccess をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 26 日 02:02 UTC
- 編集日時: 2019 年 5 月 15 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSEnhancedMonitoringRole

説明 : Cloudwatch for RDS Enhanced Monitoring へのアクセスを提供します

AmazonRDSEnhancedMonitoringRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSEnhancedMonitoringRole をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 11 日 19:58 UTC
- 編集日時: 2015 年 11 月 11 日 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSFullAccess

説明： 経由で Amazon RDS へのフルアクセスを提供します AWS Management Console。

AmazonRDSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 17 日 23:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSPerformanceInsightsFullAccess

説明： 経由で RDS Performance Insights へのフルアクセスを提供します AWS Management Console

AmazonRDSPerformanceInsightsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSPerformanceInsightsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 15 日 23:41 UTC
- 編集日時: 2023 年 10 月 23 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
    "Effect" : "Allow",
    "Action" : [
      "pi:DescribeDimensionKeys",
      "pi:GetDimensionKeyDetails",
      "pi:GetResourceMetadata",
      "pi:GetResourceMetrics",
      "pi:ListAvailableResourceDimensions",
      "pi:ListAvailableResourceMetrics"
    ],
    "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsAnalysisReportFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "pi>CreatePerformanceAnalysisReport",
      "pi:GetPerformanceAnalysisReport",
      "pi:ListPerformanceAnalysisReports",
      "pi>DeletePerformanceAnalysisReport"
    ],
    "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
  },
  {
    "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
    "Effect" : "Allow",
    "Action" : [
      "pi:TagResource",
      "pi:UntagResource",
      "pi:ListTagsForResource"
    ],
    "Resource" : "arn:aws:pi:*:*:*/*/rds/*"
  },
  {
    "Sid" : "AmazonRDSDescribeInstanceAccess",
    "Effect" : "Allow",
    "Action" : [
      "rds:DescribeDBInstances",
      "rds:DescribeDBClusters"
    ],
    "Resource" : "*"
  }
]
```

```
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSPerformanceInsightsReadOnly

説明 : RDS Performance Insights の読み取り専用ポリシー

AmazonRDSPerformanceInsightsReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSPerformanceInsightsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 5 日 00:02 UTC
- 編集日時: 2023 年 10 月 23 日 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSPreviewServiceRolePolicy

説明： Amazon RDS プレビューサービスロールポリシー

AmazonRDSPreviewServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 31 日 18:02 UTC
- 編集日時: 2023 年 10 月 4 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSReadOnlyAccess

説明： 経由で Amazon RDS への読み取り専用アクセスを提供します AWS Management Console。

AmazonRDSReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRDSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 4 月 14 日 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

}

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRDSServiceRolePolicy

説明： Amazon RDS がユーザーに代わって AWS リソースを管理できるようにします。

AmazonRDSServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 18:17 UTC
- 編集日時: 2024 年 1 月 19 日 15:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftAllCommandsFullAccess

説明：このポリシーには、Amazon Redshift でデータをコピー、ロード、アンロード、クエリ、分析するための SQL コマンドを実行するアクセス許可が含まれています。また、このポリシーは、Amazon S3、Amazon ログ、Amazon、または SageMaker AWS Glue などの関連サービスの Select ステートメントを実行するアクセス許可も付与します。CloudWatch

AmazonRedshiftAllCommandsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftAllCommandsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 4 日 00:48 UTC
- 編集日時: 2021 年 11 月 25 日 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftDataFullAccess

説明：このポリシーは、Amazon Redshift Data APIsへのフルアクセスを提供します。このポリシーは、その他の必要なサービスへのスコープ付きアクセスも付与します。

AmazonRedshiftDataFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftDataFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 9 日 19:23 UTC
- 編集日時: 2023 年 4 月 7 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftFullAccess

説明： 経由で Amazon Redshift へのフルアクセスを提供します AWS Management Console。

AmazonRedshiftFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 7 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftQueryEditor

説明 : Amazon Redshift クエリエディタと、経由で保存されたクエリへのフルアクセスを提供します AWS Management Console。

AmazonRedshiftQueryEditor は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 4 日 22:50 UTC
- 編集日時: 2021 年 2 月 16 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftQueryEditorV2FullAccess

説明： Amazon Redshift クエリエディタ V2 オペレーションとリソースへのフルアクセスを許可します。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターの一覧表示、AWS KMS でのキーとエイリアスの読み取り、AWS Secrets Manager でのクエリエディタ V2 シークレットの管理のためのアクセス許可が含まれます。

AmazonRedshiftQueryEditorV2FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:06 UTC
- 編集日時: 2024 年 2 月 21 日 17:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftQueryEditorV2NoSharing

説明： リソースを共有せずに Amazon Redshift クエリエディタ V2 を操作する機能を付与します。権限を与えられたプリンシパルは、そのリソースの読み取り、更新、削除のみが可能で、共有はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、Secrets Manager でプリンシパルのクエリエディタ V2 AWS シークレットを管理するアクセス許可が含まれます。

AmazonRedshiftQueryEditorV2NoSharing は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2NoSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:18 UTC
- 編集日時: 2024 年 2 月 21 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:user}"
    }
  }
},
{
  "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}"
  }
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftQueryEditorV2ReadSharing

説明：リソースの共有が制限された Amazon Redshift クエリエディタ V2 を操作する機能を付与します。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、チームと共有されているリソースの読み取りはできますが、更新はできません。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、Secrets Manager でプリンシパルのクエリエディタ V2 AWS シークレットを管理するアクセス許可が含まれます。

AmazonRedshiftQueryEditorV2ReadSharing は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2ReadSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:22 UTC
- 編集日時: 2024 年 2 月 21 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

説明： リソースの共有で Amazon Redshift クエリエディタ V2 を操作する機能を付与します。付与されたプリンシパルは、そのリソースを読み取り、書き込み、共有することができます。付与されたプリンシパルは、そのチームと共有されているリソースを読み取り、更新することができます。このポリシーは、その他の必要なサービスへのアクセス権限も付与します。これには、Amazon Redshift クラスターを一覧表示し、Secrets Manager でプリンシパルのクエリエディタ V2 AWS シークレットを管理するアクセス許可が含まれます。

AmazonRedshiftQueryEditorV2ReadWriteSharing は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftQueryEditorV2ReadWriteSharing をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 24 日 14:25 UTC
- 編集日時: 2024 年 2 月 21 日 17:30 UTC

- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:user}"
        }
      }
    }
  ],
  {
```

```
"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" : "AmazonRedshiftQueryEditorV20ownerSpecificPermissions",
  "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}"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftReadOnlyAccess

説明： 経由で Amazon Redshift への読み取り専用アクセスを提供します AWS Management Console。

AmazonRedshiftReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRedshiftReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 2 月 8 日 00:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRedshiftServiceLinkedRolePolicy

説明： Amazon Redshift がユーザーに代わって AWS サービスを呼び出すことを許可します

AmazonRedshiftServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 19:19 UTC
- 編集日時: 2024 年 3 月 15 日 20:00 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRekognitionCustomLabelsFullAccess

説明: このポリシーは、Amazon Rekognition Custom Labels 機能に必要な rekognition および s3 アクセス許可を指定します。

AmazonRekognitionCustomLabelsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionCustomLabelsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 1 月 8 日 19:18 UTC
- 編集日時: 2022 年 8 月 16 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRekognitionFullAccess

説明：すべての Amazon Rekognition APIs へのアクセス

AmazonRekognitionFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 14:40 UTC
- 編集日時: 2016 年 11 月 30 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRekognitionReadOnlyAccess

説明：すべての読み取り rekognition APIs へのアクセス

AmazonRekognitionReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 30 日 14:58 UTC
- 編集日時: 2023 年 11 月 8 日 18:30 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRekognitionServiceRole

説明： Rekognition がユーザーに代わって AWS サービスを呼び出すことを許可します。

AmazonRekognitionServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRekognitionServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 16:52 UTC

- 編集日時: 2017 年 11 月 29 日 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53AutoNamingFullAccess

説明：すべての Route 53 Auto Naming アクションへのフルアクセスを提供します。

AmazonRoute53AutoNamingFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 1 月 18 日 18:40 UTC
- 編集日時: 2018 年 1 月 18 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53AutoNamingReadOnlyAccess

説明：すべての Route 53 Auto Naming アクションへの読み取り専用アクセスを提供します。

AmazonRoute53AutoNamingReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 1 月 18 日 03:02 UTC
- 編集日時: 2018 年 1 月 18 日 03:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53AutoNamingRegistrantAccess

説明： Route 53 Auto Naming アクションへの登録者レベルのアクセスを提供します。

AmazonRoute53AutoNamingRegistrantAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53AutoNamingRegistrantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 12 日 22:33 UTC
- 編集日時: 2018 年 3 月 12 日 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53DomainsFullAccess

説明: すべての Route53 ドメインアクションへのフルアクセスとホストゾーンの作成を提供し、ドメイン登録の一部としてホストゾーンを作成できるようにします。

AmazonRoute53DomainsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53DomainsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53DomainsReadOnlyAccess

説明：Route53 ドメインのリストとアクションへのアクセスを提供します。

AmazonRoute53DomainsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53DomainsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ]
    }
  ]
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53FullAccess

説明： 経由ですべての Amazon Route 53 へのフルアクセスを提供します AWS Management Console。

AmazonRoute53FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 12 月 20 日 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53ProfilesFullAccess

説明：このポリシーは、Amazon Route 53 Profile リソースへのフルアクセスを許可します。

AmazonRoute53ProfilesFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ProfilesFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 30 日 18:30 UTC
- 編集日時: 2024 年 4 月 30 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "route53profiles:AssociateProfile",
  "route53profiles:AssociateResourceToProfile",
  "route53profiles:CreateProfile",
  "route53profiles>DeleteProfile",
  "route53profiles:DisassociateProfile",
  "route53profiles:DisassociateResourceFromProfile",
  "route53profiles:GetProfile",
  "route53profiles:GetProfileAssociation",
  "route53profiles:GetProfileResourceAssociation",
  "route53profiles:ListProfileAssociations",
  "route53profiles:ListProfileResourceAssociations",
  "route53profiles:ListProfiles",
  "route53profiles:ListTagsForResource",
  "route53profiles:TagResource",
  "route53profiles:UntagResource",
  "route53profiles:UpdateProfileResourceAssociation",
  "route53resolver:GetFirewallConfig",
  "route53resolver:GetFirewallRuleGroup",
  "route53resolver:GetResolverConfig",
  "route53resolver:GetResolverDnssecConfig",
  "route53resolver:GetResolverQueryLogConfig",
  "route53resolver:GetResolverRule",
  "ec2:DescribeVpcs",
  "route53:GetHostedZone"
],
"Resource" : [
  "*"
]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53ProfilesReadOnlyAccess

説明：このポリシーは、Amazon Route 53 Profile リソースへの読み取り専用アクセスを許可します。

AmazonRoute53ProfilesReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ProfilesReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 30 日 18:29 UTC
- 編集日時: 2024 年 4 月 30 日 18:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",

```

```
    "route53profiles:ListProfileResourceAssociations",
    "route53profiles:ListProfiles",
    "route53profiles:ListTagsForResource",
    "route53resolver:GetFirewallConfig",
    "route53resolver:GetResolverConfig",
    "route53resolver:GetResolverDnssecConfig",
    "route53resolver:GetResolverQueryLogConfig"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53ReadOnlyAccess

説明： 経由ですべての Amazon Route 53 への読み取り専用アクセスを提供します AWS Management Console。

AmazonRoute53ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2016 年 11 月 15 日 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryClusterFullAccess

説明 : Amazon Route 53 Recovery クラスターへのフルアクセスを提供します

AmazonRoute53RecoveryClusterFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryClusterFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:37 UTC
- 編集日時: 2021 年 8 月 18 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

説明： Amazon Route 53 Recovery クラスターへの読み取り専用アクセスを提供します

AmazonRoute53RecoveryClusterReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryClusterReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 17:36 UTC
- 編集日時: 2022 年 4 月 1 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ]
    }
  ]
}
```



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryControlConfigFullAccess

説明 : Amazon Route 53 Recovery Control Config へのフルアクセスを提供します

AmazonRoute53RecoveryControlConfigFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryControlConfigFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 17:48 UTC
- 編集日時: 2021 年 8 月 18 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

説明： Amazon Route 53 Recovery Control Config への読み取り専用アクセスを提供します

AmazonRoute53RecoveryControlConfigReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryControlConfigReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:01 UTC

- 編集日時: 2023 年 10 月 18 日 17:15 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonRoute53RecoveryControlConfigReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryReadinessFullAccess

説明： Amazon Route 53 Recovery Readiness へのフルアクセスを提供します

AmazonRoute53RecoveryReadinessFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryReadinessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 16:45 UTC
- 編集日時: 2021 年 8 月 18 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "route53-recovery-readiness:*"
],
"Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

説明： Amazon Route 53 Recovery Readiness への読み取り専用アクセスを提供します

AmazonRoute53RecoveryReadinessReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53RecoveryReadinessReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 18 日 18:11 UTC
- 編集日時: 2021 年 11 月 9 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53ResolverFullAccess

説明： Route 53 Resolver のフルアクセスポリシー

AmazonRoute53ResolverFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ResolverFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 30 日 18:10 UTC
- 編集日時: 2020 年 7 月 17 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonRoute53ResolverReadOnlyAccess

説明 : Route 53 Resolver の読み取り専用ポリシー

AmazonRoute53ResolverReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonRoute53ResolverReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 30 日 18:11 UTC
- 編集日時: 2019 年 9 月 27 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonS3FullAccess

説明： 経由ですべてのバケットへのフルアクセスを提供します AWS Management Console。

AmazonS3FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2021 年 9 月 27 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "s3-object-lambda:*"  
  ],  
  "Resource" : "*"   
}   
]   
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonS3ObjectLambdaExecutionRolePolicy

説明： Amazon S3 Object AWS Lambda とやり取りするための Lambda 関数のアクセス許可を提供します。また、ログに書き込むためのアクセス許可を Lambda CloudWatch に付与します。

AmazonS3ObjectLambdaExecutionRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3ObjectLambdaExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 18 日 10:07 UTC
- 編集日時: 2021 年 8 月 18 日 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonS3OutpostsFullAccess

説明： 経由で Amazon S3 on Outposts へのフルアクセスを提供します AWS Management Console。

AmazonS3OutpostsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3OutpostsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 2 日 17:26 UTC
- 編集日時: 2020 年 10 月 2 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonS3OutpostsReadOnlyAccess

説明： 経由で Amazon S3 on Outposts への読み取り専用アクセスを提供します AWS Management Console。

AmazonS3OutpostsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3OutpostsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 2 日 18:55 UTC

- 編集日時: 2020 年 10 月 2 日 18:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonS3ReadOnlyAccess

説明： 経由ですべてのバケットへの読み取り専用アクセスを提供します AWS Management Console。

AmazonS3ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonS3ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 8 月 10 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオから製品をプロビジョニングするために AWS のサービス Catalog サービスで使用されるサービスロールポリシー。CodePipeline、CodeBuild、CodeCommitGlue CloudFormationなどの一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 27 日 18:48 UTC
- 編集日時: 2024 年 6 月 12 日 18:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:sagemaker-*"
    ]
  },
  {
    "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:*:*:sagemaker-*"
    ]
  },
  {
    "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasAIServicesAccess

説明： Amazon SageMaker Canvas が AI サービスを使用して、すぐに使用できる AI ソリューションをサポートするためのアクセス許可を提供します。このポリシーは、Amazon SageMaker Canvas がサポートを追加するにつれて、サービスに対する変更許可を追加します。

AmazonSageMakerCanvasAIServicesAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasAIServicesAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 23 日 22:36 UTC
- 編集日時: 2023 年 11 月 29 日 14:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
```

```
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Rekognition",
    "Effect" : "Allow",
    "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Comprehend",
    "Effect" : "Allow",
    "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Bedrock",
    "Effect" : "Allow",
    "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
    ],
    "Resource" : "*"
},
{
    "Sid" : "CreateBedrockResourcesPermission",
    "Effect" : "Allow",
    "Action" : [
```

```
    "bedrock:CreateModelCustomizationJob",
    "bedrock:CreateProvisionedModelThroughput",
    "bedrock:TagResource"
  ],
  "Resource" : [
    "arn:aws:bedrock:*:*:model-customization-job/*",
    "arn:aws:bedrock:*:*:custom-model/*",
    "arn:aws:bedrock:*:*:provisioned-model/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "SageMaker",
        "Canvas"
      ]
    },
    "StringEquals" : {
      "aws:RequestTag/SageMaker" : "true",
      "aws:RequestTag/Canvas" : "true",
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceTag/Canvas" : "true"
    }
  }
},
{
  "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
  "Effect" : "Allow",
  "Action" : [
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetCustomModel",
    "bedrock:GetProvisionedModelThroughput",
    "bedrock:StopModelCustomizationJob",
    "bedrock>DeleteProvisionedModelThroughput"
  ],
  "Resource" : [
    "arn:aws:bedrock:*:*:model-customization-job/*",
    "arn:aws:bedrock:*:*:custom-model/*",
    "arn:aws:bedrock:*:*:provisioned-model/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SageMaker" : "true",
      "aws:ResourceTag/Canvas" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "FoundationModelPermission",
    "Effect" : "Allow",
    "Action" : [
      "bedrock:CreateModelCustomizationJob"
    ],
    "Resource" : [
      "arn:aws:bedrock:*::foundation-model/*"
    ]
  },
  {
    "Sid" : "BedrockFineTuningPassRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "bedrock.amazonaws.com"
      }
    }
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasBedrockAccess

説明：このポリシーは、S3 SageMaker などのダウンストリームサービスへのアクセスを提供することで、Canvas で Amazon Bedrock を使用するアクセス許可を付与します。

AmazonSageMakerCanvasBedrockAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasBedrockAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 2 月 2 日 18:37 UTC
- 編集日時: 2024 年 2 月 2 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasDataPrepFullAccess

説明：Canvas でのデータ準備のための Amazon SageMaker リソースとオペレーションへのフルアクセスを提供します。このポリシーは、関連サービス (S3、IAM、KMS、RDS、CloudWatch Logs、Redshift、Athena、Glue EventBridge、Secrets Manager など) への選択アクセスも提供します。このポリシーは、Amazon SageMaker ドメイン/ユーザープロファイル実行ロールにアタッチする必要があります。

AmazonSageMakerCanvasDataPrepFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasDataPrepFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 10 月 27 日 22:56 UTC
- 編集日時: 2023 年 12 月 8 日 02:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroup0operation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroup0operations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJob0operations",
      "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:*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasDirectDeployAccess

説明 : Amazon SageMaker Canvas が Canvas で作成されたエンドポイントのエンドポイント詳細を作成、管理、表示できるようにします。Amazon SageMaker Canvas が からエンドポイント呼び出しメトリクスを取得できるようにします CloudWatch。

AmazonSageMakerCanvasDirectDeployAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasDirectDeployAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 10 月 6 日 18:11 UTC
- 編集日時: 2023 年 10 月 6 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasForecastAccess

説明：このポリシーは、Amazon Forecast で Canvas SageMaker を使用するために一般的に必要なアクセス許可を付与します。

AmazonSageMakerCanvasForecastAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasForecastAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 8 月 24 日 20:04 UTC
- 編集日時: 2022 年 8 月 24 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCanvasFullAccess

説明： Amazon SageMaker Canvas のリソースとオペレーションへのフルアクセスを提供します。このポリシーは、関連サービス (S3、IAM、VPC、ECR、CloudWatch Logs、Redshift、Secrets

Manager、Forecast など) への選択アクセスも提供します。このポリシーは、Amazon SageMaker ドメイン/ユーザープロファイル実行ロールにアタッチする必要があります。

AmazonSageMakerCanvasFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerCanvasFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 9 日 00:44 UTC
- 編集日時: 2024 年 1 月 24 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerClusterInstanceRolePolicy

説明：このポリシーは、Amazon SageMaker クラスターを使用するために一般的に必要なアクセス許可を付与します。

AmazonSageMakerClusterInstanceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerClusterInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 15:11 UTC
- 編集日時: 2023 年 11 月 29 日 15:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerCoreServiceRolePolicy

説明： Amazon SageMaker Core Services のサービスにリンクされたロールの管理ポリシー

AmazonSageMakerCoreServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 21 日 21:40 UTC
- 編集日時: 2020 年 12 月 21 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerEdgeDeviceFleetPolicy

説明 : SageMaker Edge がデフォルトのクラウド接続を使用してお客様のデバイスフリートを作成および管理するために必要なアクセス許可を提供します。

AmazonSageMakerEdgeDeviceFleetPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerEdgeDeviceFleetPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 8 日 16:17 UTC
- 編集日時: 2020 年 12 月 8 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerFeatureStoreAccess

説明： Amazon SageMaker FeatureStore 特徴量グループのオフラインストアを有効にするために必要なアクセス許可を提供します。

AmazonSageMakerFeatureStoreAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFeatureStoreAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 16:24 UTC
- 編集日時: 2022 年 12 月 5 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerFullAccess

説明：AWS Management Console および SDK SageMaker 経由で Amazon へのフルアクセスを提供します。また、関連サービス (S3、ECR、CloudWatch Logs など) への選択アクセスも提供します。

AmazonSageMakerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集日時: 2024 年 3 月 29 日 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v26 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    }
  ],
  {
```



```
"Sid" : "AllowAddTagsForSpace",
"Effect" : "Allow",
"Action" : [
  "sagemaker:AddTags"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:space/*"
],
"Condition" : {
  "StringEquals" : {
    "sagemaker:TaggingAction" : "CreateSpace"
  }
}
},
{
  "Sid" : "AllowAddTagsForApp",
"Effect" : "Allow",
"Action" : [
  "sagemaker:AddTags"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:app/*"
]
},
{
  "Sid" : "AllowStudioActions",
"Effect" : "Allow",
"Action" : [
  "sagemaker:CreatePresignedDomainUrl",
  "sagemaker:DescribeDomain",
  "sagemaker:ListDomains",
  "sagemaker:DescribeUserProfile",
  "sagemaker:ListUserProfiles",
  "sagemaker:DescribeSpace",
  "sagemaker:ListSpaces",
  "sagemaker:DescribeApp",
  "sagemaker:ListApps"
],
"Resource" : "*"
},
{
  "Sid" : "AllowAppActionsForUserProfile",
"Effect" : "Allow",
"Action" : [
```

```
    "sagemaker:CreateApp",
    "sagemaker>DeleteApp"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
  "Condition" : {
    "Null" : {
      "sagemaker:OwnerUserProfileArn" : "true"
    }
  }
},
{
  "Sid" : "AllowAppActionsForSharedSpaces",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateApp",
    "sagemaker>DeleteApp"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*/*",
  "Condition" : {
    "StringEquals" : {
      "sagemaker:SpaceSharingType" : [
        "Shared"
      ]
    }
  }
},
{
  "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateSpace",
    "sagemaker:UpdateSpace",
    "sagemaker>DeleteSpace"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
  "Condition" : {
    "Null" : {
      "sagemaker:OwnerUserProfileArn" : "true"
    }
  }
},
{
  "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
  "Effect" : "Allow",
```

```

    "Action" : [
      "sagemaker:CreateSpace",
      "sagemaker:UpdateSpace",
      "sagemaker>DeleteSpace"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private",
          "Shared"
        ]
      }
    }
  },
  {
    "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
    "Effect" : "Allow",
    "Action" : [
      "sagemaker>CreateApp",
      "sagemaker>DeleteApp"
    ],
    "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition" : {
      "ArnLike" : {
        "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
      },
      "StringEquals" : {
        "sagemaker:SpaceSharingType" : [
          "Private"
        ]
      }
    }
  },
  {
    "Sid" : "AllowFlowDefinitionActions",
    "Effect" : "Allow",
    "Action" : "sagemaker:*",
    "Resource" : [

```

```
    "arn:aws:sagemaker:*:*:flow-definition/*"
  ],
  "Condition" : {
    "StringEqualsIfExists" : {
      "sagemaker:WorkteamType" : [
        "private-crowd",
        "vendor-crowd"
      ]
    }
  }
},
{
  "Sid" : "AllowAWSServiceActions",
  "Effect" : "Allow",
  "Action" : [
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "cognito-idp:AdminAddUserToGroup",
    "cognito-idp:AdminCreateUser",
    "cognito-idp:AdminDeleteUser",
    "cognito-idp:AdminDisableUser",
    "cognito-idp:AdminEnableUser",
    "cognito-idp:AdminRemoveUserFromGroup",
```

```
"cognito-idp:CreateGroup",
"cognito-idp:CreateUserPool",
"cognito-idp:CreateUserPoolClient",
"cognito-idp:CreateUserPoolDomain",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:List*",
"cognito-idp:UpdateUserPool",
"cognito-idp:UpdateUserPoolClient",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateVpcEndpoint",
"ec2>DeleteNetworkInterface",
"ec2>DeleteNetworkInterfacePermission",
"ec2:DescribeDhcpOptions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:CreateRepository",
"ecr:Describe*",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:StartImageScan",
"elastic-inference:Connect",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeMountTargets",
"fsx:DescribeFileSystems",
"glue:CreateJob",
"glue>DeleteJob",
"glue:GetJob*",
"glue:GetTable*",
"glue:GetWorkflowRun",
"glue:ResetJobBookmark",
"glue:StartJobRun",
"glue:StartWorkflowRun",
"glue:UpdateJob",
"groundtruthlabeling:*",
"iam:ListRoles",
"kms:DescribeKey",
```

```
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery",
    "robomaker:CreateSimulationApplication",
    "robomaker:DescribeSimulationApplication",
    "robomaker>DeleteSimulationApplication",
    "robomaker:CreateSimulationJob",
    "robomaker:DescribeSimulationJob",
    "robomaker:CancelSimulationJob",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowECRActions",
  "Effect" : "Allow",
  "Action" : [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr>DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr>DeleteRepository",
    "ecr:PutImage"
  ],
  "Resource" : [
```

```
    "arn:aws:ecr:*:*:repository/*sagemaker*"
  ]
},
{
  "Sid" : "AllowCodeCommitActions",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:GitPull",
    "codecommit:GitPush"
  ],
  "Resource" : [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
  ]
},
{
  "Sid" : "AllowCodeBuildActions",
  "Action" : [
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
  ],
  "Resource" : [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
  ],
  "Effect" : "Allow"
},
{
  "Sid" : "AllowStepFunctionsActions",
  "Action" : [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
  ],
  "Resource" : [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
    "arn:aws:states:*:*:execution:*sagemaker*:*"
  ],
  "Effect" : "Allow"
},
{
```

```
"Sid" : "AllowSecretManagerActions",
"Effect" : "Allow",
"Action" : [
  "secretsmanager:DescribeSecret",
  "secretsmanager:GetSecretValue",
  "secretsmanager:CreateSecret"
],
"Resource" : [
  "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
]
},
{
  "Sid" : "AllowReadOnlySecretManagerActions",
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "secretsmanager:ResourceTag/SageMaker" : "true"
    }
  }
},
{
  "Sid" : "AllowServiceCatalogProvisionProduct",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:ProvisionProduct"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "servicecatalog:userLevel" : "self"
    }
  }
}
```



```
    }
  }
},
{
  "Sid" : "AllowS3ObjectActions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*",
    "arn:aws:s3::*aws-glue*"
  ]
},
{
  "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*"
  ],
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "s3:ExistingObjectTag/SageMaker" : "true"
    }
  }
},
{
  "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*"
  ],
  "Condition" : {
```

```
    "StringEquals" : {
      "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
    }
  },
  {
    "Sid" : "AllowS3BucketActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:GetBucketCors",
      "s3:PutBucketCors"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AllowS3BucketACL",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketAcl",
      "s3:PutObjectAcl"
    ],
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Sid" : "AllowLambdaInvokeFunction",
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : [
      "arn:aws:lambda::*:function:*SageMaker*",
      "arn:aws:lambda::*:function:*sagemaker*",
      "arn:aws:lambda::*:function:*Sagemaker*",
      "arn:aws:lambda::*:function:*LabelingFunction*"
    ]
  },
}
```

```
{
  "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
  "Action" : "iam:CreateServiceLinkedRole",
  "Effect" : "Allow",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "robomaker.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowSNSActions",
  "Effect" : "Allow",
  "Action" : [
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish"
  ],
  "Resource" : [
    "arn:aws:sns::*::*SageMaker*",
    "arn:aws:sns::*::*Sagemaker*",
    "arn:aws:sns::*::*sagemaker*"
  ]
},
{
  "Sid" : "AllowPassRoleForSageMakerRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
```

```
"Condition" : {
  "StringEquals" : {
    "iam:PassedToService" : [
      "glue.amazonaws.com",
      "robomaker.amazonaws.com",
      "states.amazonaws.com"
    ]
  }
},
{
  "Sid" : "AllowPassRoleToSageMaker",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "sagemaker.amazonaws.com"
    }
  }
},
{
  "Sid" : "AllowAthenaActions",
  "Effect" : "Allow",
  "Action" : [
    "athena:ListDataCatalogs",
    "athena:ListDatabases",
    "athena:ListTableMetadata",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:StartQueryExecution",
    "athena:StopQueryExecution"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowGlueCreateTable",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateTable"
```

```
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
      "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*"
    ]
  },
  {
    "Sid" : "AllowGlueUpdateTable",
    "Effect" : "Allow",
    "Action" : [
      "glue:UpdateTable"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/sagemaker_featurestore"
    ]
  },
  {
    "Sid" : "AllowGlueDeleteTable",
    "Effect" : "Allow",
    "Action" : [
      "glue>DeleteTable"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*"
    ]
  },
  {
    "Sid" : "AllowGlueGetTablesAndDatabases",
    "Effect" : "Allow",
    "Action" : [
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:table/*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*"
    ]
  }
}
```

```
]
},
{
  "Sid" : "AllowGlueGetAndCreateDatabase",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateDatabase",
    "glue:GetDatabase"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/sagemaker_featurestore",
    "arn:aws:glue:*:*:database/sagemaker_processing",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
  ]
},
{
  "Sid" : "AllowRedshiftDataActions",
  "Effect" : "Allow",
  "Action" : [
    "redshift-data:ExecuteStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:CancelStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AllowRedshiftGetClusterCredentials",
  "Effect" : "Allow",
  "Action" : [
    "redshift:GetClusterCredentials"
  ],
  "Resource" : [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
  ]
},
{
```

```
"Sid" : "AllowListTagsForUserProfile",
"Effect" : "Allow",
"Action" : [
  "sagemaker:ListTags"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:user-profile/*"
],
},
{
  "Sid" : "AllowCloudformationListStackResources",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ListStackResources"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
  "Sid" : "AllowS3ExpressObjectActions",
  "Effect" : "Allow",
  "Action" : [
    "s3express:CreateSession"
  ],
  "Resource" : [
    "arn:aws:s3express:*:*:bucket/*SageMaker*",
    "arn:aws:s3express:*:*:bucket/*Sagemaker*",
    "arn:aws:s3express:*:*:bucket/*sagemaker*",
    "arn:aws:s3express:*:*:bucket/*aws-gluue*"
  ],
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerGeospatialExecutionRole

説明：このポリシーは、SageMaker 地理空間の使用に一般的に必要なサービスへのアクセスを提供します。

AmazonSageMakerGeospatialExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGeospatialExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 11 月 30 日 10:08 UTC
- 編集日時: 2023 年 5 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerGeospatialFullAccess

説明：このポリシーは、AWS Management Console および SDK を介して Amazon SageMaker Geospatial へのフルアクセスを許可するアクセス許可を付与します。

AmazonSageMakerGeospatialFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGeospatialFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 11 月 30 日 10:06 UTC
- 編集日時: 2022 年 11 月 30 日 10:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerGroundTruthExecution

説明： SageMaker GroundTruth ラベル付けジョブの実行に必要な AWS サービスへのアクセスを提供します

AmazonSageMakerGroundTruthExecution は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerGroundTruthExecution をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 9 日 19:30 UTC
- 編集日時: 2022 年 4 月 29 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerMechanicalTurkAccess

説明: 任意の Workteam に対して Amazon Augmented AI FlowDefinition リソースを作成するためのアクセスを提供します。

AmazonSageMakerMechanicalTurkAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerMechanicalTurkAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 16:19 UTC
- 編集日時: 2019 年 12 月 3 日 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerModelGovernanceUseAccess

説明：この AWS 管理ポリシーは、すべての Amazon SageMaker Governance 機能を使用するために必要なアクセス許可を付与します。このポリシーは、関連サービス (S3、KMS など) への限定アクセスも提供します。

AmazonSageMakerModelGovernanceUseAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerModelGovernanceUseAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 30 日 08:58 UTC
- 編集日時: 2024 年 6 月 4 日 21:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker>DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
```

```
    "sagemaker:ListModelCardExportJobs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowSMTrainingModelsSearchTags",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:ListTrainingJobs",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:ListModels",
    "sagemaker:DescribeModel",
    "sagemaker:Search",
    "sagemaker:AddTags",
    "sagemaker>DeleteTags",
    "sagemaker:ListTags"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowKMSActions",
  "Effect" : "Allow",
  "Action" : [
    "kms:ListAliases"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowS3Actions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:CreateBucket",
    "s3:GetBucketLocation"
  ],
  "Resource" : [
    "arn:aws:s3::*SageMaker*",
    "arn:aws:s3::*Sagemaker*",
    "arn:aws:s3::*sagemaker*"
  ]
},
{
  "Sid" : "AllowS3ListActions",
```

```
    "Effect" : "Allow",
    "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerModelRegistryFullAccess

説明：これは Sagemaker の Model Registry の新しいマネージドポリシーです。このポリシーは、ユーザーロールにアタッチして Sagemaker のモデルレジストリ関連の機能にアクセスできるスタンドアロンポリシーです。

AmazonSageMakerModelRegistryFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerModelRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 13 日 05:20 UTC
- 編集日時: 2024 年 6 月 6 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",

```

```
    "sagemaker:DeleteModelPackage",
    "sagemaker:DeleteModelPackageGroup",
    "sagemaker:DeleteTags",
    "sagemaker:UpdateModelPackage"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::*SageMaker*",
    "arn:aws:s3:::*Sagemaker*",
    "arn:aws:s3:::*sagemaker*"
  ]
},
{
  "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:DescribeImages"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/*",
```

```
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "sagemaker.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:GetGroupQuery"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:CreateGroup",
      "resource-groups:Tag"
    ],
    "Resource" : "arn:aws:resource-groups:*:*:group/*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : "sagemaker:collection"
      }
    }
  }
},
```

```
{
  "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
  "Effect" : "Allow",
  "Action" : "resource-groups:DeleteGroup",
  "Resource" : "arn:aws:resource-groups:*:*:group/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker:collection" : "true"
    }
  }
},
{
  "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource" : "arn:aws:kms:*:*:key/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/sagemaker" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "sagemaker.*.amazonaws.com"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerNotebooksServiceRolePolicy

説明： Amazon SageMaker Notebooks のサービスにリンクされたロールの管理ポリシー

AmazonSageMakerNotebooksServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 18 日 20:27 UTC
- 編集日時: 2024 年 5 月 22 日 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
```

```
        "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
        "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
    }
}
},
{
    "Sid" : "AllowEFSAccessPointDeletion",
    "Effect" : "Allow",
    "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
    ],
    "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
{
    "Sid" : "AllowEFSCreation",
    "Effect" : "Allow",
    "Action" : "elasticfilesystem:CreateFileSystem",
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
{
    "Sid" : "AllowEFSMountWithDeletion",
    "Effect" : "Allow",
    "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem>DeleteFileSystem",
        "elasticfilesystem>DeleteMountTarget"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringLike" : {
            "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
    }
},
}
```

```
{
  "Sid" : "AllowEFSDescribe",
  "Effect" : "Allow",
  "Action" : [
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowEFSTagging",
  "Effect" : "Allow",
  "Action" : "elasticfilesystem:TagResource",
  "Resource" : [
    "arn:aws:elasticfilesystem:*:*:access-point/*",
    "arn:aws:elasticfilesystem:*:*:file-system/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Sid" : "AllowEC2Tagging",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*"
  ]
},
{
  "Sid" : "AllowEC2Operations",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
```

```
    "ec2:DescribeVpcs",
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowEC2AuthZ",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateNetworkInterfacePermission",
    "ec2>DeleteNetworkInterfacePermission",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
    }
  }
},
{
  "Sid" : "AllowIdcOperations",
  "Effect" : "Allow",
  "Action" : [
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteManagedApplicationInstance",
    "sso:GetManagedApplicationInstance"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowSagemakerProfileCreation",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:CreateUserProfile",
    "sagemaker:DescribeUserProfile"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "AllowSageMakerSpaceOperationsForCanvasManagedSpaces",
"Effect" : "Allow",
"Action" : [
  "sagemaker:CreateSpace",
  "sagemaker:DescribeSpace",
  "sagemaker>DeleteSpace",
  "sagemaker:ListTags"
],
"Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
},
{
  "Sid" : "AllowSageMakerAddTagsForAppManagedSpaces",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddTags"
  ],
  "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
  "Condition" : {
    "StringEquals" : {
      "sagemaker:TaggingAction" : "CreateSpace"
    }
  }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS APIGateway によって使用されるサービスロールポリシー。Lambda などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC
- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品 AWS CloudFormation 内で によって使用されるサービスロールポリシー。Lambda、APIGateway などの関連サービスのサブセットにアクセス許可を付与します。

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:06 UTC
- 編集日時: 2023 年 8 月 1 日 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS Lambda が使用するサービスロールポリシー。Secrets Manager などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 1 日 15:05 UTC
- 編集日時: 2023 年 8 月 1 日 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerPipelinesIntegrations

説明: この Amazon 管理ポリシーは、SageMaker モデル構築パイプラインのコールバックステップと Lambda ステップで使用するために一般的に必要なアクセス許可を付与します。これはに追加され、SageMaker Studio の設定時に作成 AmazonSageMakerExecutionRole できます。パイプラインの作成または実行に使用される他のロールにアタッチすることもできます。

AmazonSageMakerPipelinesIntegrations は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerPipelinesIntegrations をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 7 月 30 日 16:35 UTC
- 編集日時: 2023 年 2 月 17 日 21:28 UTC

- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerReadOnly

説明： AWS Management Console および SDK SageMaker 経由で Amazon への読み取り専用アクセスを提供します。

AmazonSageMakerReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 13:07 UTC
- 編集日時: 2021 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS APIGateway によって使用されるサービスロールポリシー。CloudWatch ログなど、一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 3 月 25 日 04:25 UTC
- 編集日時: 2022 年 3 月 25 日 04:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品 AWS CloudFormation 内で によって使用されるサービスロールポリシー。およびその他を含む関連サービスのサブセットにアクセス許可を付与 SageMaker します。

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 3 月 25 日 04:26 UTC
- 編集日時: 2022 年 3 月 25 日 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品 AWS CodeBuild 内で、よって使用されるサービスロールポリシー。など CodePipeline、関連サービスのサブセットにアクセス許可を付与 CodeBuild します。

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 3 月 25 日 04:27 UTC
- 編集日時: 2024 年 6 月 11 日 18:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "codecommit:CancelUploadArchive",
  "codecommit:GetBranch",
  "codecommit:GetCommit",
  "codecommit:GetUploadArchiveStatus",
  "codecommit:UploadArchive"
],
"Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
},
{
  "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:DescribeImageScanFindings",
    "ecr:DescribeRegistry",
    "ecr:DescribeImageReplicationStatus",
    "ecr:DescribeRepositories",
    "ecr:DescribeImageReplicationStatus",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
  "Effect" : "Allow",
  "Action" : [
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart"
  ],
  "Resource" : [
    "arn:aws:ecr:*:*:repository/sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerCodeBuildPassRolePermission",
  "Effect" : "Allow",
```

```
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "events.amazonaws.com",
          "codepipeline.amazonaws.com",
          "cloudformation.amazonaws.com",
          "codebuild.amazonaws.com",
          "sagemaker.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AmazonSageMakerCodeBuildLogPermission",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogDelivery",
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs>DeleteLogDelivery",
      "logs:DescribeLogGroups",
      "logs:DescribeLogStreams",
      "logs:DescribeResourcePolicies",
      "logs:DescribeDestinations",
      "logs:DescribeExportTasks",
      "logs:DescribeMetricFilters",
      "logs:DescribeQueries",
      "logs:DescribeQueryDefinitions",
      "logs:DescribeSubscriptionFilters",
```

```
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
},
{
  "Sid" : "AmazonSageMakerCodeBuildS3Permission",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3>DeleteBucket",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:PutBucketCors",
    "s3:AbortMultipartUpload",
    "s3>DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
```

```
"sagemaker:CreateAction",
"sagemaker:CreateAlgorithm",
"sagemaker:CreateApp",
"sagemaker:CreateAppImageConfig",
"sagemaker:CreateArtifact",
"sagemaker:CreateAutoMLJob",
"sagemaker:CreateCodeRepository",
"sagemaker:CreateCompilationJob",
"sagemaker:CreateContext",
"sagemaker:CreateDataQualityJobDefinition",
"sagemaker:CreateDeviceFleet",
"sagemaker:CreateDomain",
"sagemaker:CreateEdgePackagingJob",
"sagemaker:CreateEndpoint",
"sagemaker:CreateEndpointConfig",
"sagemaker:CreateExperiment",
"sagemaker:CreateFeatureGroup",
"sagemaker:CreateFlowDefinition",
"sagemaker:CreateHumanTaskUi",
"sagemaker:CreateHyperParameterTuningJob",
"sagemaker:CreateImage",
"sagemaker:CreateImageVersion",
"sagemaker:CreateInferenceRecommendationsJob",
"sagemaker:CreateLabelingJob",
"sagemaker:CreateLineageGroupPolicy",
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
```



```
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker>DeleteAction",
"sagemaker>DeleteAlgorithm",
"sagemaker>DeleteApp",
"sagemaker>DeleteAppImageConfig",
"sagemaker>DeleteArtifact",
"sagemaker>DeleteAssociation",
"sagemaker>DeleteCodeRepository",
"sagemaker>DeleteContext",
"sagemaker>DeleteDataQualityJobDefinition",
"sagemaker>DeleteDeviceFleet",
"sagemaker>DeleteDomain",
"sagemaker>DeleteEndpoint",
"sagemaker>DeleteEndpointConfig",
"sagemaker>DeleteExperiment",
"sagemaker>DeleteFeatureGroup",
"sagemaker>DeleteFlowDefinition",
"sagemaker>DeleteHumanLoop",
"sagemaker>DeleteHumanTaskUi",
"sagemaker>DeleteImage",
"sagemaker>DeleteImageVersion",
"sagemaker>DeleteLineageGroupPolicy",
"sagemaker>DeleteModel",
"sagemaker>DeleteModelBiasJobDefinition",
"sagemaker>DeleteModelExplainabilityJobDefinition",
"sagemaker>DeleteModelPackage",
"sagemaker>DeleteModelPackageGroup",
"sagemaker>DeleteModelPackageGroupPolicy",
"sagemaker>DeleteModelQualityJobDefinition",
"sagemaker>DeleteMonitoringSchedule",
"sagemaker>DeleteNotebookInstance",
"sagemaker>DeleteNotebookInstanceLifecycleConfig",
"sagemaker>DeletePipeline",
"sagemaker>DeleteProject",
"sagemaker>DeleteRecord",
"sagemaker>DeleteTags",
"sagemaker>DeleteTrial",
"sagemaker>DeleteTrialComponent",
"sagemaker>DeleteUserProfile",
"sagemaker>DeleteWorkforce",
"sagemaker>DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
```

```
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
```

```
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
```

```
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
"sagemaker:ListTrials",
"sagemaker:ListUserProfiles",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
```

```
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:endpoint/*",
  "arn:aws:sagemaker:*:*:endpoint-config/*",
  "arn:aws:sagemaker:*:*:model/*",
  "arn:aws:sagemaker:*:*:pipeline/*",
  "arn:aws:sagemaker:*:*:project/*",
```

```
    "arn:aws:sagemaker:*:*:model-package/*"
  ],
},
{
  "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*"
  ],
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "aws:ResourceTag/sagemaker" : "true"
    }
  }
},
{
  "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
  "Effect" : "Allow",
  "Action" : [
    "codeconnections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codeconnections:*:*:connection/*"
  ],
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "aws:ResourceTag/sagemaker" : "true"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品 AWS CodePipeline 内で、よって使用されるサービスロールポリシー。など CodePipeline、関連サービスのサブセットにアクセス許可を付与 CodeBuild します。

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2024 年 6 月 11 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "cloudformation:CreateChangeSet",
  "cloudformation:CreateStack",
  "cloudformation:DescribeChangeSet",
  "cloudformation>DeleteChangeSet",
  "cloudformation>DeleteStack",
  "cloudformation:DescribeStacks",
  "cloudformation:ExecuteChangeSet",
  "cloudformation:SetStackPolicy",
  "cloudformation:UpdateStack"
],
"Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
},
{
  "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "sagemaker:project-name"
      ]
    }
  }
},
{
  "Sid" : "AmazonSageMakerCodePipelineS3Permission",
  "Effect" : "Allow",
  "Action" : [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3::*:sagemaker-*"
  ]
},
{
```



```
    "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
    ]
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
    "Effect" : "Allow",
    "Action" : [
      "codebuild:BatchGetBuilds",
      "codebuild:StartBuild"
    ],
    "Resource" : [
      "arn:aws:codebuild::*:project/sagemaker-*",
      "arn:aws:codebuild::*:build/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
    "Effect" : "Allow",
    "Action" : [
      "codecommit:CancelUploadArchive",
      "codecommit:GetBranch",
      "codecommit:GetCommit",
      "codecommit:GetUploadArchiveStatus",
      "codecommit:UploadArchive"
    ],
    "Resource" : "arn:aws:codecommit::*:sagemaker-*"
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
      "codestar-connections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codestar-connections::*:connection/*"
    ],
    "Condition" : {
```

```
    "StringEqualsIgnoreCase" : {
      "aws:ResourceTag/sagemaker" : "true"
    }
  },
  {
    "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
    "Effect" : "Allow",
    "Action" : [
      "codeconnections:UseConnection"
    ],
    "Resource" : [
      "arn:aws:codeconnections:*:*:connection/*"
    ],
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "aws:ResourceTag/sagemaker" : "true"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内の AWS CloudWatch イベントで使用されるサービスロールポリシー。およびその他を含む関連サービスのサブセットにアクセス許可を付与 CodePipeline します。

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:53 UTC
- 編集日時: 2022 年 2 月 22 日 09:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS Firehose が使用するサービスロールポリシー。Firehose などを含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:54 UTC
- 編集日時: 2022 年 2 月 22 日 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS Glue が使用するサービスロールポリシー。このポリシーは、Glue やその他を含めた一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 2 月 22 日 09:51 UTC
- 編集日時: 2022 年 8 月 26 日 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

説明: Amazon 製品 SageMaker ポートフォリオの AWS ServiceCatalog プロビジョニング済み製品内で AWS Lambda が使用するサービスロールポリシー。ECR、S3、その他を含む一連の関連サービスにアクセス許可を付与します。

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 4 日 16:34 UTC
- 編集日時: 2024 年 6 月 11 日 18:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr>DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ],
```

```
    "Resource" : [
      "arn:aws:ecr:*:*:repository/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
    "Effect" : "Allow",
    "Action" : [
      "events:DeleteRule",
      "events:DescribeRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource" : [
      "arn:aws:events:*:*:rule/sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
    "Effect" : "Allow",
    "Action" : [
      "s3:CreateBucket",
      "s3:DeleteBucket",
      "s3:GetBucketAcl",
      "s3:GetBucketCors",
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads",
      "s3:PutBucketCors"
    ],
    "Resource" : [
      "arn:aws:s3:::aws-glue-*",
      "arn:aws:s3:::sagemaker-*"
    ]
  },
  {
    "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
    "Effect" : "Allow",
    "Action" : [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:GetObject",
```

```
    "s3:GetObjectVersion",
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-glue-*",
    "arn:aws:s3:::sagemaker-*"
  ]
},
{
  "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
  "Effect" : "Allow",
  "Action" : [
    "sagemaker:AddAssociation",
    "sagemaker:AddTags",
    "sagemaker:AssociateTrialComponent",
    "sagemaker:BatchDescribeModelPackage",
    "sagemaker:BatchGetMetrics",
    "sagemaker:BatchGetRecord",
    "sagemaker:BatchPutMetrics",
    "sagemaker:CreateAction",
    "sagemaker:CreateAlgorithm",
    "sagemaker:CreateApp",
    "sagemaker:CreateAppImageConfig",
    "sagemaker:CreateArtifact",
    "sagemaker:CreateAutoMLJob",
    "sagemaker:CreateCodeRepository",
    "sagemaker:CreateCompilationJob",
    "sagemaker:CreateContext",
    "sagemaker:CreateDataQualityJobDefinition",
    "sagemaker:CreateDeviceFleet",
    "sagemaker:CreateDomain",
    "sagemaker:CreateEdgePackagingJob",
    "sagemaker:CreateEndpoint",
    "sagemaker:CreateEndpointConfig",
    "sagemaker:CreateExperiment",
    "sagemaker:CreateFeatureGroup",
    "sagemaker:CreateFlowDefinition",
    "sagemaker:CreateHumanTaskUi",
    "sagemaker:CreateHyperParameterTuningJob",
    "sagemaker:CreateImage",
    "sagemaker:CreateImageVersion",
    "sagemaker:CreateInferenceRecommendationsJob",
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateLineageGroupPolicy",
```

```
"sagemaker:CreateModel",
"sagemaker:CreateModelBiasJobDefinition",
"sagemaker:CreateModelExplainabilityJobDefinition",
"sagemaker:CreateModelPackage",
"sagemaker:CreateModelPackageGroup",
"sagemaker:CreateModelQualityJobDefinition",
"sagemaker:CreateMonitoringSchedule",
"sagemaker:CreateNotebookInstance",
"sagemaker:CreateNotebookInstanceLifecycleConfig",
"sagemaker:CreatePipeline",
"sagemaker:CreatePresignedDomainUrl",
"sagemaker:CreatePresignedNotebookInstanceUrl",
"sagemaker:CreateProcessingJob",
"sagemaker:CreateProject",
"sagemaker:CreateTrainingJob",
"sagemaker:CreateTransformJob",
"sagemaker:CreateTrial",
"sagemaker:CreateTrialComponent",
"sagemaker:CreateUserProfile",
"sagemaker:CreateWorkforce",
"sagemaker:CreateWorkteam",
"sagemaker:DeleteAction",
"sagemaker:DeleteAlgorithm",
"sagemaker:DeleteApp",
"sagemaker:DeleteAppImageConfig",
"sagemaker:DeleteArtifact",
"sagemaker:DeleteAssociation",
"sagemaker:DeleteCodeRepository",
"sagemaker:DeleteContext",
"sagemaker:DeleteDataQualityJobDefinition",
"sagemaker:DeleteDeviceFleet",
"sagemaker:DeleteDomain",
"sagemaker:DeleteEndpoint",
"sagemaker:DeleteEndpointConfig",
"sagemaker:DeleteExperiment",
"sagemaker:DeleteFeatureGroup",
"sagemaker:DeleteFlowDefinition",
"sagemaker:DeleteHumanLoop",
"sagemaker:DeleteHumanTaskUi",
"sagemaker:DeleteImage",
"sagemaker:DeleteImageVersion",
"sagemaker:DeleteLineageGroupPolicy",
"sagemaker:DeleteModel",
"sagemaker:DeleteModelBiasJobDefinition",
```

```
"sagemaker:DeleteModelExplainabilityJobDefinition",
"sagemaker:DeleteModelPackage",
"sagemaker:DeleteModelPackageGroup",
"sagemaker:DeleteModelPackageGroupPolicy",
"sagemaker:DeleteModelQualityJobDefinition",
"sagemaker:DeleteMonitoringSchedule",
"sagemaker:DeleteNotebookInstance",
"sagemaker:DeleteNotebookInstanceLifecycleConfig",
"sagemaker:DeletePipeline",
"sagemaker:DeleteProject",
"sagemaker:DeleteRecord",
"sagemaker:DeleteTags",
"sagemaker:DeleteTrial",
"sagemaker:DeleteTrialComponent",
"sagemaker:DeleteUserProfile",
"sagemaker:DeleteWorkforce",
"sagemaker:DeleteWorkteam",
"sagemaker:DeregisterDevices",
"sagemaker:DescribeAction",
"sagemaker:DescribeAlgorithm",
"sagemaker:DescribeApp",
"sagemaker:DescribeAppImageConfig",
"sagemaker:DescribeArtifact",
"sagemaker:DescribeAutoMLJob",
"sagemaker:DescribeCodeRepository",
"sagemaker:DescribeCompilationJob",
"sagemaker:DescribeContext",
"sagemaker:DescribeDataQualityJobDefinition",
"sagemaker:DescribeDevice",
"sagemaker:DescribeDeviceFleet",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEdgePackagingJob",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeExperiment",
"sagemaker:DescribeFeatureGroup",
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanLoop",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeHyperParameterTuningJob",
"sagemaker:DescribeImage",
"sagemaker:DescribeImageVersion",
"sagemaker:DescribeInferenceRecommendationsJob",
"sagemaker:DescribeLabelingJob",
```

```
"sagemaker:DescribeLineageGroup",
"sagemaker:DescribeModel",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelExplainabilityJobDefinition",
"sagemaker:DescribeModelPackage",
"sagemaker:DescribeModelPackageGroup",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeMonitoringSchedule",
"sagemaker:DescribeNotebookInstance",
"sagemaker:DescribeNotebookInstanceLifecycleConfig",
"sagemaker:DescribePipeline",
"sagemaker:DescribePipelineDefinitionForExecution",
"sagemaker:DescribePipelineExecution",
"sagemaker:DescribeProcessingJob",
"sagemaker:DescribeProject",
"sagemaker:DescribeSubscribedWorkteam",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeTransformJob",
"sagemaker:DescribeTrial",
"sagemaker:DescribeTrialComponent",
"sagemaker:DescribeUserProfile",
"sagemaker:DescribeWorkforce",
"sagemaker:DescribeWorkteam",
"sagemaker:DisableSagemakerServicecatalogPortfolio",
"sagemaker:DisassociateTrialComponent",
"sagemaker:EnableSagemakerServicecatalogPortfolio",
"sagemaker:GetDeviceFleetReport",
"sagemaker:GetDeviceRegistration",
"sagemaker:GetLineageGroupPolicy",
"sagemaker:GetModelPackageGroupPolicy",
"sagemaker:GetRecord",
"sagemaker:GetSagemakerServicecatalogPortfolioStatus",
"sagemaker:GetSearchSuggestions",
"sagemaker:InvokeEndpoint",
"sagemaker:InvokeEndpointAsync",
"sagemaker:ListActions",
"sagemaker:ListAlgorithms",
"sagemaker:ListAppImageConfigs",
"sagemaker:ListApps",
"sagemaker:ListArtifacts",
"sagemaker:ListAssociations",
"sagemaker:ListAutoMLJobs",
"sagemaker:ListCandidatesForAutoMLJob",
"sagemaker:ListCodeRepositories",
```

```
"sagemaker:ListCompilationJobs",
"sagemaker:ListContexts",
"sagemaker:ListDataQualityJobDefinitions",
"sagemaker:ListDeviceFleets",
"sagemaker:ListDevices",
"sagemaker:ListDomains",
"sagemaker:ListEdgePackagingJobs",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListEndpoints",
"sagemaker:ListExperiments",
"sagemaker:ListFeatureGroups",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanLoops",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListHyperParameterTuningJobs",
"sagemaker:ListImageVersions",
"sagemaker:ListImages",
"sagemaker:ListInferenceRecommendationsJobs",
"sagemaker:ListLabelingJobs",
"sagemaker:ListLabelingJobsForWorkteam",
"sagemaker:ListLineageGroups",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelExplainabilityJobDefinitions",
"sagemaker:ListModelMetadata",
"sagemaker:ListModelPackageGroups",
"sagemaker:ListModelPackages",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListModels",
"sagemaker:ListMonitoringExecutions",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListNotebookInstanceLifecycleConfigs",
"sagemaker:ListNotebookInstances",
"sagemaker:ListPipelineExecutionSteps",
"sagemaker:ListPipelineExecutions",
"sagemaker:ListPipelineParametersForExecution",
"sagemaker:ListPipelines",
"sagemaker:ListProcessingJobs",
"sagemaker:ListProjects",
"sagemaker:ListSubscribedWorkteams",
"sagemaker:ListTags",
"sagemaker:ListTrainingJobs",
"sagemaker:ListTrainingJobsForHyperParameterTuningJob",
"sagemaker:ListTransformJobs",
"sagemaker:ListTrialComponents",
```

```
"sagemaker:ListTrials",
"sagemaker:ListUserProfile",
"sagemaker:ListWorkforces",
"sagemaker:ListWorkteams",
"sagemaker:PutLineageGroupPolicy",
"sagemaker:PutModelPackageGroupPolicy",
"sagemaker:PutRecord",
"sagemaker:QueryLineage",
"sagemaker:RegisterDevices",
"sagemaker:RenderUiTemplate",
"sagemaker:Search",
"sagemaker:SendHeartbeat",
"sagemaker:SendPipelineExecutionStepFailure",
"sagemaker:SendPipelineExecutionStepSuccess",
"sagemaker:StartHumanLoop",
"sagemaker:StartMonitoringSchedule",
"sagemaker:StartNotebookInstance",
"sagemaker:StartPipelineExecution",
"sagemaker:StopAutoMLJob",
"sagemaker:StopCompilationJob",
"sagemaker:StopEdgePackagingJob",
"sagemaker:StopHumanLoop",
"sagemaker:StopHyperParameterTuningJob",
"sagemaker:StopInferenceRecommendationsJob",
"sagemaker:StopLabelingJob",
"sagemaker:StopMonitoringSchedule",
"sagemaker:StopNotebookInstance",
"sagemaker:StopPipelineExecution",
"sagemaker:StopProcessingJob",
"sagemaker:StopTrainingJob",
"sagemaker:StopTransformJob",
"sagemaker:UpdateAction",
"sagemaker:UpdateAppImageConfig",
"sagemaker:UpdateArtifact",
"sagemaker:UpdateCodeRepository",
"sagemaker:UpdateContext",
"sagemaker:UpdateDeviceFleet",
"sagemaker:UpdateDevices",
"sagemaker:UpdateDomain",
"sagemaker:UpdateEndpoint",
"sagemaker:UpdateEndpointWeightsAndCapacities",
"sagemaker:UpdateExperiment",
"sagemaker:UpdateImage",
"sagemaker:UpdateModelPackage",
```



```
"sagemaker:UpdateMonitoringSchedule",
"sagemaker:UpdateNotebookInstance",
"sagemaker:UpdateNotebookInstanceLifecycleConfig",
"sagemaker:UpdatePipeline",
"sagemaker:UpdatePipelineExecution",
"sagemaker:UpdateProject",
"sagemaker:UpdateTrainingJob",
"sagemaker:UpdateTrial",
"sagemaker:UpdateTrialComponent",
"sagemaker:UpdateUserProfile",
"sagemaker:UpdateWorkforce",
"sagemaker:UpdateWorkteam"
],
"Resource" : [
  "arn:aws:sagemaker:*:*:action/*",
  "arn:aws:sagemaker:*:*:algorithm/*",
  "arn:aws:sagemaker:*:*:app-image-config/*",
  "arn:aws:sagemaker:*:*:artifact/*",
  "arn:aws:sagemaker:*:*:automl-job/*",
  "arn:aws:sagemaker:*:*:code-repository/*",
  "arn:aws:sagemaker:*:*:compilation-job/*",
  "arn:aws:sagemaker:*:*:context/*",
  "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
  "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
  "arn:aws:sagemaker:*:*:device-fleet/*",
  "arn:aws:sagemaker:*:*:edge-packaging-job/*",
  "arn:aws:sagemaker:*:*:endpoint/*",
  "arn:aws:sagemaker:*:*:endpoint-config/*",
  "arn:aws:sagemaker:*:*:experiment/*",
  "arn:aws:sagemaker:*:*:experiment-trial/*",
  "arn:aws:sagemaker:*:*:experiment-trial-component/*",
  "arn:aws:sagemaker:*:*:feature-group/*",
  "arn:aws:sagemaker:*:*:human-loop/*",
  "arn:aws:sagemaker:*:*:human-task-ui/*",
  "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
  "arn:aws:sagemaker:*:*:image/*",
  "arn:aws:sagemaker:*:*:image-version/*/*",
  "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
  "arn:aws:sagemaker:*:*:labeling-job/*",
  "arn:aws:sagemaker:*:*:model/*",
  "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
  "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
  "arn:aws:sagemaker:*:*:model-package/*",
  "arn:aws:sagemaker:*:*:model-package-group/*",
```

```
    "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
    "arn:aws:sagemaker:*:*:monitoring-schedule/*",
    "arn:aws:sagemaker:*:*:notebook-instance/*",
    "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
    "arn:aws:sagemaker:*:*:pipeline/*",
    "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
    "arn:aws:sagemaker:*:*:processing-job/*",
    "arn:aws:sagemaker:*:*:project/*",
    "arn:aws:sagemaker:*:*:training-job/*",
    "arn:aws:sagemaker:*:*:transform-job/*",
    "arn:aws:sagemaker:*:*:workforce/*",
    "arn:aws:sagemaker:*:*:workteam/*"
  ]
},
{
  "Sid" : "AmazonSageMakerLambdaPassRolePermission",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam:*:*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
  ]
},
{
  "Sid" : "AmazonSageMakerLambdaLogPermission",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs>DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:DescribeResourcePolicies",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeMetricFilters",
    "logs:DescribeQueries",
    "logs:DescribeQueryDefinitions",
    "logs:DescribeSubscriptionFilters",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
```

```
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:PutResourcePolicy",
    "logs:UpdateLogDelivery"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
},
{
  "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:StartBuild",
    "codebuild:BatchGetBuilds"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/sagemaker:project-name" : "*"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSecurityLakeAdministrator

説明： Security Lake の管理に必要な Amazon Security Lake および関連サービスへのフルアクセスを提供します。

AmazonSecurityLakeAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AmazonSecurityLakeAdministrator` をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 30 日 22:04 UTC
- 編集日時: 2024 年 2 月 23 日 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSecurityLakeMetastoreManager

説明 : cloudwatch、S3、Glue、SQS へのアクセスを許可する Amazon SecurityLake メタストアマネージャーの Lambda のポリシー。

AmazonSecurityLakeMetastoreManager は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakeMetastoreManager をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2024 年 1 月 23 日 15:26 UTC
- 編集日時: 2024 年 4 月 1 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
```



```
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
},
{
    "Sid" : "AllowGlueManage",
    "Effect" : "Allow",
    "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
    ],
    "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/**",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db**",
        "arn:aws:glue:*:*:catalog"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}
},
{
    "Sid" : "AllowToReadFromSqs",
    "Effect" : "Allow",
    "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes"
    ],
    "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}
},
{
    "Sid" : "AllowMetaDataReadWrite",
    "Effect" : "Allow",
```

```
"Action" : [
  "s3:ListBucket",
  "s3:PutObject",
  "s3:GetObject"
],
"Resource" : [
  "arn:aws:s3:::aws-security-data-lake*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "AllowMetaDataCleanup",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
    "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSecurityLakePermissionsBoundary

説明: Amazon Security Lake は、データレイクにデータを書き込むためのサードパーティーのカスタムソースと、データレイクからデータを使用するためのサードパーティーのサブスクライバーの IAM ロールを作成し、これらのロールを作成するときにこのポリシーを使用してアクセス許可の境界を定義します。

AmazonSecurityLakePermissionsBoundary は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSecurityLakePermissionsBoundary をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 29 日 14:11 UTC
- 編集日時: 2024 年 5 月 14 日 20:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation",
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DenyActionsForSecurityLake",
  "Effect" : "Deny",
  "NotAction" : [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation",
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DenyActionsNotOnSecurityLakeBucket",
  "Effect" : "Deny",
  "Action" : [
    "s3:GetObject",
```

```
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation"
  ],
  "NotResource" : [
    "arn:aws:s3:::aws-security-data-lake*"
  ]
},
{
  "Sid" : "DenyActionsNotOnSecurityLakeSQS",
  "Effect" : "Deny",
  "Action" : [
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
  "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringNotLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com",
        "sqs.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
  "Effect" : "Deny",
```

```
"Action" : [
  "kms:Decrypt",
  "kms:GenerateDataKey"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "kms:EncryptionContext:aws:s3:arn" : "false"
  },
  "StringNotLikeIfExists" : {
    "kms:EncryptionContext:aws:s3:arn" : [
      "arn:aws:s3:::aws-security-data-lake*"
    ]
  }
}
},
{
  "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
  "Effect" : "Deny",
  "Action" : [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "kms:EncryptionContext:aws:sqs:arn" : "false"
    },
    "StringNotLikeIfExists" : {
      "kms:EncryptionContext:aws:sqs:arn" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSESEFullAccess

説明： 経由で Amazon SES へのフルアクセスを提供します AWS Management Console。

AmazonSESEFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSESEFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESEFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSESReadOnlyAccess

説明： 経由で Amazon SES への読み取り専用アクセスを提供します AWS Management Console。

AmazonSESReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSESReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 5 月 14 日 12:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSESServiceRolePolicy

説明 : SES が SES リソースに代わって Amazon CloudWatch 基本モニタリングメトリクスを発行することを許可する

AmazonSESServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 5 月 21 日 16:02 UTC
- 編集日時: 2024 年 5 月 21 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSNSFullAccess

説明： 経由で Amazon SNS へのフルアクセスを提供します AWS Management Console。

AmazonSNSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSNSReadOnlyAccess

説明： 経由で Amazon SNS への読み取り専用アクセスを提供します AWS Management Console。

AmazonSNSReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSNSRole

説明： Amazon SNS サービスロールのデフォルトポリシー。

AmazonSNSRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSNSRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC

- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSQSFullAccess

説明： 経由で Amazon SQS へのフルアクセスを提供します AWS Management Console。

AmazonSQSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSQSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSQSReadOnlyAccess

説明： 経由で Amazon SQS への読み取り専用アクセスを提供します AWS Management Console。

AmazonSQSReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSQSReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 5 月 24 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
"Sid" : "AmazonSQSReadOnlyAccess",
"Effect" : "Allow",
"Action" : [
  "sqs:GetQueueAttributes",
  "sqs:GetQueueUrl",
  "sqs:ListDeadLetterSourceQueues",
  "sqs:ListQueues",
  "sqs:ListMessageMoveTasks",
  "sqs:ListQueueTags"
],
"Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMAutomationApproverAccess

説明：自動化の実行を表示し、承認待ちの自動化に承認決定を送信するアクセスを提供します

AmazonSSMAutomationApproverAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 7 日 23:07 UTC
- 編集日時: 2017 年 8 月 7 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMAutomationRole

説明： EC2 Automation サービスが Automation ドキュメント内で定義されたアクティビティを実行するためのアクセス許可を付与します

AmazonSSMAutomationRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMAutomationRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 5 日 22:09 UTC
- 編集日時: 2017 年 7 月 24 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMDirectoryServiceAccess

説明：このポリシーは、SSM エージェントがお客様に代わって Directory Service にアクセスして、マネージドインスタンスにドメイン参加することを許可します。

AmazonSSMDirectoryServiceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMDirectoryServiceAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 3 月 15 日 17:44 UTC
- 編集日時: 2019 年 3 月 15 日 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMFullAccess

説明： Amazon SSM へのフルアクセスを提供します。

AmazonSSMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 29 日 17:39 UTC
- 編集日時: 2019 年 11 月 20 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMMaintenanceWindowRole

説明: EC2 メンテナンスウィンドウに使用されるサービスロール

AmazonSSMMaintenanceWindowRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMMaintenanceWindowRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 1 日 15:57 UTC
- 編集日時: 2019 年 7 月 27 日 00:16 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:ListGroupResources",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSSManagedEC2InstanceDefaultPolicy

説明：このポリシーは、EC2 インスタンスで AWS Systems Manager 機能を有効にします。

AmazonSSManagedEC2InstanceDefaultPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMManagedEC2InstanceDefaultPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 30 日 20:54 UTC
- 編集日時: 2022 年 8 月 30 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMManagedInstanceCore

説明 : AWS Systems Manager サービスコア機能を有効にする Amazon EC2 ロールのポリシー。

AmazonSSMManagedInstanceCore は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMManagedInstanceCore をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 3 月 15 日 17:22 UTC
- 編集日時: 2019 年 5 月 23 日 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMPatchAssociation

説明：パッチの関連付け操作のために子インスタンスへのアクセスを提供します。

AmazonSSMPatchAssociation は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMPatchAssociation をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 13 日 16:00 UTC
- 編集日時: 2020 年 5 月 13 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMReadOnlyAccess

説明 : Amazon SSM への読み取り専用アクセスを提供します。

AmazonSSMReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSSMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 29 日 17:44 UTC
- 編集日時: 2015 年 5 月 29 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonSSMServiceRolePolicy

説明： Amazon SSM が管理または使用する AWS リソースへのアクセスを提供します

AmazonSSMServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 13 日 19:20 UTC
- 編集日時: 2022 年 9 月 14 日 19:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonSumerianFullAccess

説明： Amazon Sumerian へのフルアクセスを提供します。

AmazonSumerianFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonSumerianFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 24 日 20:14 UTC
- 編集日時: 2018 年 4 月 24 日 20:14 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonTextractFullAccess

説明 : すべての Amazon Textract APIs へのアクセス

AmazonTextractFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTextextractFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 19:07 UTC
- 編集日時: 2018 年 11 月 28 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextextractFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonTextractServiceRole

説明： Textract がユーザーに代わって AWS サービスを呼び出すことを許可します。

AmazonTextractServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTextractServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 28 日 19:12 UTC
- 編集日時: 2018 年 11 月 28 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Resource" : "arn:aws:sns:*:*:AmazonTexttract*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonTimestreamConsoleFullAccess

説明： を使用して Amazon Timestream を管理するためのフルアクセスを提供します AWS Management Console。このポリシーでは、特定の KMS オペレーションや、保存したクエリを管理する操作に対するアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

AmazonTimestreamConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2022 年 2 月 1 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonTimestreamFullAccess

説明： Amazon Timestream へのフルアクセスを提供します。このポリシーでは、特定の KMS オペレーションへのアクセス許可も付与されることに注意してください。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

AmazonTimestreamFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2021 年 11 月 26 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonTimestreamInfluxDBFullAccess

説明: Amazon Timestream InfluxDB インスタンスを作成、更新、削除、一覧表示し、パラメータグループを作成、一覧表示するための完全な管理アクセスを提供します。必要な追加のアクセス許可については、「ドキュメント」を参照してください。

AmazonTimestreamInfluxDBFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamInfluxDBFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 14 日 22:53 UTC
- 編集日時: 2024 年 3 月 14 日 22:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonTimestreamInfluxDBServiceRolePolicy

説明: Amazon Timestream InfluxDB インスタンスを作成、更新、削除、一覧表示し、パラメータグループを作成、一覧表示するための完全な管理アクセスを提供します。必要な追加のアクセス許可については、「ドキュメント」を参照してください。

AmazonTimestreamInfluxDBServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 3 月 14 日 18:53 UTC
- 編集日時: 2024 年 3 月 14 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonTimestreamReadOnlyAccess

説明： Amazon Timestream への読み取り専用アクセスを提供します。ポリシーには、実行中のクエリをキャンセルするアクセス許可も付与されます。カスタマー管理型 CMK を使用している場合は、必要な追加のアクセス許可についてドキュメントを参照してください。

AmazonTimestreamReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTimestreamReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC
- 編集日時: 2024 年 6 月 5 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AmazonTimestreamReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "timestream:CancelQuery",
      "timestream:DescribeDatabase",
      "timestream:DescribeEndpoints",
      "timestream:DescribeTable",
      "timestream:ListDatabases",
      "timestream:ListMeasures",
      "timestream:ListTables",
      "timestream:ListTagsForResource",
      "timestream:Select",
      "timestream:SelectValues",
      "timestream:DescribeScheduledQuery",
      "timestream:ListScheduledQueries",
      "timestream:DescribeBatchLoadTask",
      "timestream:ListBatchLoadTasks",
      "timestream:DescribeAccountSettings"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonTranscribeFullAccess

説明 : Amazon Transcribe オペレーションへのフルアクセスを提供します

AmazonTranscribeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTranscribeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 16:06 UTC
- 編集日時: 2018 年 4 月 4 日 16:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3::*transcribe*"
      ]
    }
  ]
}
```



```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonTranscribeReadOnlyAccess

説明： Amazon Transcribe の読み取り専用オペレーションへのアクセスを提供します

AmazonTranscribeReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonTranscribeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 16:05 UTC
- 編集日時: 2018 年 4 月 4 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

説明： ネットワークインターフェイスを作成し、クロスアカウントリソースにアタッチするためのアクセスを提供します

AmazonVPCCrossAccountNetworkInterfaceOperations は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCCrossAccountNetworkInterfaceOperations をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 7 月 18 日 20:47 UTC

- 編集日時: 2023 年 9 月 25 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCCrossAccountNetworkInterfaceOperations

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCFullAccess

説明： 経由で Amazon VPC へのフルアクセスを提供します AWS Management Console。

AmazonVPCFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 2 月 8 日 16:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

説明 : AWS リソースを記述し、Network Access Analyzer を実行し、Network Insights アクセススコープと Network Insights アクセススコープ分析でタグを作成または削除するためのアクセス許可を提供します。

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCNetworkAccessAnalyzerFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 15 日 22:56 UTC

- 編集日時：2024 年 5 月 15 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2>DeleteNetworkInsightsAccessScope",
        "ec2>DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
    "ec2:DescribeNetworkInsightsAccessScopes",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
    "ec2:GetNetworkInsightsAccessScopeContent",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "ec2:StartNetworkInsightsAccessScopeAnalysis"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2TagsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-access-scope/*",
    "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
  ]
},
```

```
{
  "Sid" : "ElasticloadbalancingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GlobalacceleratorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "Sid" : "NetworkFirewallPermissions",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups"
  ],
  "Resource" : "*"
},
{
```

```
    "Sid" : "ResourceGroupsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "resource-groups:ListGroupResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TagsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "TirosPermissions",
    "Effect" : "Allow",
    "Action" : [
      "tiros:CreateQuery",
      "tiros:GetQueryAnswer"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

説明：AWS リソースを記述し、Reachability Analyzer を実行し、Network Insights パスと Network Insights Analysis でタグを作成または削除するためのアクセス許可を提供します。

AmazonVPCReachabilityAnalyzerFullAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCReachabilityAnalyzerFullAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 14 日 20:12 UTC
- 編集日時: 2024 年 5 月 15 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
  ],
}
```

```
"Sid" : "EC2Permissions",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateNetworkInsightsPath",
  "ec2>DeleteNetworkInsightsAnalysis",
  "ec2>DeleteNetworkInsightsPath",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeCustomerGateways",
  "ec2:DescribeInstances",
  "ec2:DescribeInternetGateways",
  "ec2:DescribeManagedPrefixLists",
  "ec2:DescribeNatGateways",
  "ec2:DescribeNetworkAcls",
  "ec2:DescribeNetworkInsightsAnalyses",
  "ec2:DescribeNetworkInsightsPaths",
  "ec2:DescribeNetworkInterfaces",
  "ec2:DescribePrefixLists",
  "ec2:DescribeRegions",
  "ec2:DescribeRouteTables",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSubnets",
  "ec2:DescribeTransitGatewayAttachments",
  "ec2:DescribeTransitGatewayConnects",
  "ec2:DescribeTransitGatewayPeeringAttachments",
  "ec2:DescribeTransitGatewayRouteTables",
  "ec2:DescribeTransitGateways",
  "ec2:DescribeTransitGatewayVpcAttachments",
  "ec2:DescribeVpcEndpoints",
  "ec2:DescribeVpcEndpointServiceConfigurations",
  "ec2:DescribeVpcPeeringConnections",
  "ec2:DescribeVpcs",
  "ec2:DescribeVpnConnections",
  "ec2:DescribeVpnGateways",
  "ec2:GetManagedPrefixListEntries",
  "ec2:GetTransitGatewayRouteTablePropagations",
  "ec2:SearchTransitGatewayRoutes",
  "ec2:StartNetworkInsightsAnalysis"
],
"Resource" : "*"
},
{
  "Sid" : "EC2TagsPermissions",
  "Effect" : "Allow",
  "Action" : [
```

```
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource" : [
    "arn:*:ec2:*:*:network-insights-path/*",
    "arn:*:ec2:*:*:network-insights-analysis/*"
  ]
},
{
  "Sid" : "ElasticloadbalancingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GlobalacceleratorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners"
  ],
  "Resource" : "*"
},
{
  "Sid" : "NetworkFirewallPermissions",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
```



```
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TirosPermissions",
  "Effect" : "Allow",
  "Action" : [
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

説明：このポリシーはロール IAM にアタッチされます

RoleForReachabilityAnalyzerCrossAccountResourceAccess。管理アカウントが Reachability Analyzer に対して信頼できるアクセスを有効にすると、このロールは組織のメンバーアカウントに展開されます。Reachability Analyzer コンソールを使用して組織全体のリソースを表示するためのアクセス許可を付与します。

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 5 月 1 日 20:38 UTC
- 編集日時: 2023 年 5 月 1 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonVPCReadOnlyAccess

説明： 経由で Amazon VPC への読み取り専用アクセスを提供します AWS Management Console。

AmazonVPCReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonVPCReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 2 月 8 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"

```

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkDocsFullAccess

説明： WorkDocs 経由で Amazon へのフルアクセスを提供します AWS Management Console

AmazonWorkDocsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkDocsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 16 日 23:05 UTC
- 編集日時: 2020 年 4 月 16 日 23:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkDocsReadOnlyAccess

説明： WorkDocs 経由で Amazon への読み取り専用アクセスを提供します AWS Management Console

AmazonWorkDocsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkDocsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 1 月 8 日 23:49 UTC
- 編集日時: 2020 年 1 月 8 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkMailEventsServiceRolePolicy

説明： Amazon WorkMail Events が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AmazonWorkMailEventsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 16 日 16:52 UTC
- 編集日時: 2019 年 4 月 16 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkMailFullAccess

説明： WorkMail、 Directory Service、 SES、 EC2 へのフルアクセスと KMS メタデータへの読み取りアクセスを提供します。

AmazonWorkMailFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 12 月 21 日 14:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkMailMessageFlowFullAccess

説明： WorkMail Message Flow APIsへのフルアクセス

AmazonWorkMailMessageFlowFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 11 日 11:08 UTC
- 編集日時: 2021 年 2 月 11 日 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkMailMessageFlowReadOnlyAccess

説明 : GetRawMessageContent API の WorkMail メッセージへの読み取り専用アクセス

AmazonWorkMailMessageFlowReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailMessageFlowReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 28 日 12:40 UTC
- 編集日時: 2021 年 1 月 28 日 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkMailReadOnlyAccess

説明 : WorkMail および SES への読み取り専用アクセスを提供します。

AmazonWorkMailReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkMailReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 7 月 25 日 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesAdmin

説明： AWS SDK および CLI 経由で Amazon WorkSpaces 管理アクションへのアクセスを提供します。

AmazonWorkSpacesAdmin は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 9 月 22 日 22:21 UTC
- 編集日時: 2023 年 8 月 3 日 23:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesApplicationManagerAdminAccess

説明： Amazon WorkSpaces Application Manager でアプリケーションをパッケージ化するための管理者アクセスを提供します。

AmazonWorkSpacesApplicationManagerAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesApplicationManagerAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 4 月 9 日 14:03 UTC
- 編集日時: 2015 年 4 月 9 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkspacesPCAAccess

説明：この管理ポリシーは、証明書ベースの認証 AWS アカウントのために、の AWS Certificate Manager Private CA リソースへの完全な管理アクセスを提供します。

AmazonWorkspacesPCAAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkspacesPCAAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 8 日 00:25 UTC
- 編集日時: 2022 年 11 月 8 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesSelfServiceAccess

説明 : Workspace Self Service アクションを実行するための Amazon WorkSpaces バックエンドサービスへのアクセスを提供します

AmazonWorkSpacesSelfServiceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesSelfServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 19:22 UTC
- 編集日時: 2019 年 6 月 27 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesServiceAccess

説明： Workspace を起動するための AWS WorkSpaces サービスへのお客様のアカウントアクセスを提供します。

AmazonWorkSpacesServiceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesServiceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 19:19 UTC
- 編集日時: 2020 年 3 月 18 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesWebReadOnly

説明 : 、 SDK AWS Management Console、および CLI を介して Amazon WorkSpaces Web とその依存関係への読み取り専用アクセスを提供します。

AmazonWorkSpacesWebReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonWorkSpacesWebReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 30 日 14:20 UTC
- 編集日時: 2022 年 11 月 2 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AmazonWorkSpacesWebServiceRolePolicy

説明： Amazon WorkSpaces Web が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AmazonWorkSpacesWebServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 13:15 UTC
- 編集日時: 2022 年 12 月 15 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonZocaloFullAccess

説明： Amazon Zocalo へのフルアクセスを提供します。

AmazonZocaloFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonZocaloFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmazonZocaloReadOnlyAccess

説明： Amazon Zocalo への読み取り専用アクセスを提供します

AmazonZocaloReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmazonZocaloReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```

```
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AmplifyBackendDeployFullAccess

説明: AWS クラウド Development Kit (AWS CDK) を介して Amplify バックエンドリソース (AWS AppSync、Amazon Cognito、Amazon S3、およびその他の関連サービス) をデプロイするためのフルアクセス許可を Amplify に提供します

AmplifyBackendDeployFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AmplifyBackendDeployFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 10 月 6 日 21:32 UTC
- 編集日時: 2024 年 5 月 31 日 15:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation>DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```



```
  },
  {
    "Sid" : "AmplifyHotSwappableResources",
    "Effect" : "Allow",
    "Action" : [
      "appsync:GetSchemaCreationStatus",
      "appsync:StartSchemaCreation",
      "appsync:UpdateResolver",
      "appsync:ListFunctions",
      "appsync:UpdateFunction",
      "appsync:UpdateApiKey"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AmplifyHotSwappableFunctionResource",
    "Effect" : "Allow",
    "Action" : [
      "lambda:InvokeFunction",
      "lambda:UpdateFunctionCode",
      "lambda:GetFunction",
      "lambda:UpdateFunctionConfiguration"
    ],
    "Resource" : [
      "arn:aws:lambda:*:*:function:amplify-*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "AmplifySchema",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3::*:amplify*",
      "arn:aws:s3::*:cdk-*--assets-*-*"
    ]
  },
```

```
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
},
{
  "Sid" : "CDKDeploy",
  "Effect" : "Allow",
  "Action" : [
    "sts:AssumeRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
    "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
    "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
    "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AmplifySSM",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParametersByPath",
    "ssm:GetParameters",
    "ssm:GetParameter"
  ],
  "Resource" : [
    "arn:aws:ssm::*:parameter/amplify/*",
    "arn:aws:ssm::*:parameter/cdk-bootstrap/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid" : "AmplifyModifySSMParam",
```

```
"Effect" : "Allow",
"Action" : [
  "ssm:PutParameter",
  "ssm>DeleteParameter",
  "ssm>DeleteParameters"
],
"Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "AmplifyDiscoverRDSVpcConfig",
  "Effect" : "Allow",
  "Action" : [
    "rds:DescribeDBProxies",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "ec2:DescribeSubnets",
    "rds:DescribeDBSubnetGroups"
  ],
  "Resource" : [
    "arn:aws:rds:*:*:db:*",
    "arn:aws:rds:*:*:cluster:*",
    "arn:aws:rds:*:*:db-proxy:*",
    "arn:aws:rds:*:*:subgrp:*",
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

APIGatewayServiceRolePolicy

説明： API Gateway が顧客に代わって関連する AWS リソースを管理できるようにします。

APIGatewayServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 17:23 UTC
- 編集日時: 2021 年 7 月 12 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AppIntegrationsServiceLinkedRolePolicy

説明： AppIntegrations がユーザーに代わって AppFlow リソースを管理し、 CloudWatch メトリクスデータを公開できるようにします。

AppIntegrationsServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 30 日 19:42 UTC
- 編集日時: 2022 年 9 月 30 日 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ApplicationAutoScalingForAmazonAppStreamAccess

説明: Amazon のアプリケーション自動スケーリングを有効にするポリシー AppStream

ApplicationAutoScalingForAmazonAppStreamAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ApplicationAutoScalingForAmazonAppStreamAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 6 日 21:39 UTC
- 編集日時: 2017 年 2 月 6 日 21:39 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

説明： Application Discovery Service の継続的エクスポート機能によって使用または管理される AWS のサービス およびリソースへのアクセスを有効にします

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 9 日 20:22 UTC
- 編集日時: 2018 年 8 月 13 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AppRunnerNetworkingServiceRolePolicy

説明： AWS AppRunner ネットワークがユーザーに代わって関連 AWS リソースを管理できるようにします。

AppRunnerNetworkingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 12 日 21:02 UTC
- 編集日時: 2022 年 1 月 12 日 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AppRunnerServiceRolePolicy

説明： AWS AppRunner がユーザーに代わって関連 AWS リソースを管理できるようにします。

AppRunnerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:15 UTC
- 編集日時: 2021 年 5 月 14 日 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AutoScalingConsoleFullAccess

説明： 経由で Auto Scaling へのフルアクセスを提供します AWS Management Console。

AutoScalingConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:43 UTC
- 編集日時: 2018 年 2 月 6 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AutoScalingConsoleReadOnlyAccess

説明： 経由で Auto Scaling への読み取り専用アクセスを提供します AWS Management Console。

AutoScalingConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:48 UTC
- 編集日時: 2017 年 1 月 12 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AutoScalingFullAccess

説明： Auto Scaling へのフルアクセスを提供します。

AutoScalingFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:31 UTC
- 編集日時: 2018 年 2 月 6 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AutoScalingNotificationAccessRole

説明 : AutoScaling Notification Access サービスロールのデフォルトポリシー。

AutoScalingNotificationAccessRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingNotificationAccessRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AutoScalingReadOnlyAccess

説明 : Auto Scaling への読み取り専用アクセスを提供します。

AutoScalingReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AutoScalingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 12 日 19:39 UTC
- 編集日時: 2017 年 1 月 12 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AutoScalingServiceRolePolicy

説明： Auto Scaling が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする

AutoScalingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 1 月 8 日 23:10 UTC
- 編集日時: 2024 年 2 月 29 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWS_ConfigRole

説明: AWS Config サービスロールのデフォルトポリシー。AWS Config が AWS リソースの変更を追跡するために必要なアクセス許可を提供します。

AWS_ConfigRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWS_ConfigRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 15 日 20:30 UTC
- 編集日時: 2024 年 2 月 22 日 21:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

ポリシーのバージョン

ポリシーのバージョン: v30 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",

```

```
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:ListApps",
"amplify:ListBranches",
"amplifyuibuilder:ExportThemes",
"amplifyuibuilder:GetTheme",
"amplifyuibuilder:ListThemes",
"apigateway:GET",
"app-integrations:GetEventIntegration",
"app-integrations:ListEventIntegrationAssociations",
"app-integrations:ListEventIntegrations",
"appconfig:GetApplication",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetExtensionAssociation",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListExtensionAssociations",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeFlow",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:DescribeScalableTargets",
"application-autoscaling:DescribeScalingPolicies",
"appmesh:DescribeGatewayRoute",
"appmesh:DescribeMesh",
"appmesh:DescribeRoute",
"appmesh:DescribeVirtualGateway",
"appmesh:DescribeVirtualNode",
"appmesh:DescribeVirtualRouter",
"appmesh:DescribeVirtualService",
"appmesh:ListGatewayRoutes",
"appmesh:ListMeshes",
"appmesh:ListRoutes",
"appmesh:ListTagsForResource",
```



```
"appmesh:ListVirtualGateways",
"appmesh:ListVirtualNodes",
"appmesh:ListVirtualRouters",
"appmesh:ListVirtualServices",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"appstream:DescribeApplications",
"appstream:DescribeDirectoryConfigs",
"appstream:DescribeFleets",
"appstream:DescribeStacks",
"appstream:ListTagsForResource",
"appsync:GetApiCache",
"appsync:GetGraphQLApi",
"appsync:ListGraphQLApis",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"APS:DescribeRuleGroupsNamespace",
"APS:DescribeWorkspace",
"aps:ListRuleGroupsNamespaces",
"aps:ListTagsForResource",
"APS:ListWorkspaces",
"athena:GetDataCatalog",
"athena:GetPreparedStatement",
"athena:GetWorkGroup",
"athena:ListDataCatalogs",
"athena:ListPreparedStatements",
"athena:ListTagsForResource",
"athena:ListWorkGroups",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:ListAssessments",
"autoscaling-plans:DescribeScalingPlanResources",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeLaunchConfigurations",
"autoscaling:DescribeLifecycleHooks",
"autoscaling:DescribePolicies",
"autoscaling:DescribeScheduledActions",
"autoscaling:DescribeTags",
"autoscaling:DescribeWarmPool",
```

```
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:DescribeBackupVault",
"backup:DescribeFramework",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
"backup:DescribeReportPlan",
"backup:GetBackupPlan",
"backup:GetBackupSelection",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListFrameworks",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListReportPlans",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:DescribeSchedulingPolicies",
"batch:ListSchedulingPolicies",
"batch:ListTagsForResource",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListTagsForResource",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionsForBudget",
"budgets:ViewBudget",
"cassandra:Select",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"cloud9:DescribeEnvironmentMemberships",
"cloud9:DescribeEnvironments",
"cloud9:ListEnvironments",
"cloud9:ListTagsForResource",
"cloudformation:DescribeType",
"cloudformation:GetResource",
"cloudformation:ListResources",
```

```
"cloudformation:ListStackResources",
"cloudformation:ListStacks",
"cloudformation:ListTypes",
"cloudfront:GetFunction",
"cloudfront:GetOriginAccessControl",
"cloudfront:GetResponseHeadersPolicy",
"cloudfront:ListDistributions",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListResponseHeadersPolicies",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventDataStore",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListEventDataStores",
"cloudtrail:ListTags",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:DescribeAnomalyDetectors",
"cloudwatch:GetDashboard",
"cloudwatch:GetMetricStream",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"cloudwatch:ListTagsForResource",
"codeartifact:DescribeRepository",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListTagsForResource",
"codebuild:BatchGetReportGroups",
"codebuild:ListReportGroups",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:ListRepositories",
"codecommit:ListTagsForResource",
"codedeploy:GetDeploymentConfig",
"codeguru-profiler:DescribeProfilingGroup",
"codeguru-profiler:GetNotificationConfiguration",
"codeguru-profiler:GetPolicy",
"codeguru-profiler:ListProfilingGroups",
```

```
"codeguru-reviewer:DescribeRepositoryAssociation",
"codeguru-reviewer:ListRepositoryAssociations",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"cognito-identity:DescribeIdentityPool",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetPrincipalTagAttributeMap",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:DescribeIdentityProvider",
"cognito-idp:DescribeResourceServer",
"cognito-idp:DescribeUserPool",
"cognito-idp:DescribeUserPoolClient",
"cognito-idp:DescribeUserPoolDomain",
"cognito-idp:GetGroup",
"cognito-idp:GetUserPoolMfaConfig",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"config:BatchGet*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:Put*",
"config:Select*",
"connect:DescribeEvaluationForm",
"connect:DescribeInstance",
"connect:DescribeInstanceStorageConfig",
"connect:DescribePhoneNumber",
"connect:DescribePrompt",
"connect:DescribeQuickConnect",
"connect:DescribeRule",
"connect:DescribeUser",
"connect:GetTaskTemplate",
"connect:ListApprovedOrigins",
"connect:ListEvaluationForms",
"connect:ListInstanceAttributes",
"connect:ListInstances",
"connect:ListInstanceStorageConfigs",
"connect:ListIntegrationAssociations",
```

```
"connect:ListPhoneNumbers",
"connect:ListPhoneNumbersV2",
"connect:ListPrompts",
"connect:ListQuickConnects",
"connect:ListRules",
"connect:ListSecurityKeys",
"connect:ListTagsForResource",
"connect:ListTaskTemplates",
"connect:ListUsers",
"connect:SearchAvailablePhoneNumbers",
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"datasync:DescribeAgent",
"datasync:DescribeLocationEfs",
"datasync:DescribeLocationFsxLustre",
"datasync:DescribeLocationFsxWindows",
"datasync:DescribeLocationHdfs",
"datasync:DescribeLocationNfs",
"datasync:DescribeLocationObjectStorage",
"datasync:DescribeLocationS3",
"datasync:DescribeLocationSmb",
"datasync:DescribeTask",
"datasync:ListAgents",
"datasync:ListLocations",
"datasync:ListTagsForResource",
"datasync:ListTasks",
"dax:DescribeClusters",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
"dax:ListTags",
"detective:ListGraphs",
"detective:ListTagsForResource",
```

```
"devicefarm:GetInstanceProfile",
"devicefarm:GetNetworkProfile",
"devicefarm:GetProject",
"devicefarm:GetTestGridProject",
"devicefarm>ListInstanceProfiles",
"devicefarm>ListNetworkProfiles",
"devicefarm>ListProjects",
"devicefarm>ListTagsForResource",
"devicefarm>ListTestGridProjects",
"devops-guru:GetResourceCollection",
"dms:DescribeCertificates",
"dms:DescribeEndpoints",
"dms:DescribeEventSubscriptions",
"dms:DescribeReplicationInstances",
"dms:DescribeReplicationSubnetGroups",
"dms:DescribeReplicationTaskAssessmentRuns",
"dms:DescribeReplicationTasks",
"dms>ListTagsForResource",
"ds:DescribeDirectories",
"ds:DescribeDomainControllers",
"ds:DescribeEventTopics",
"ds>ListLogSubscriptions",
"ds>ListTagsForResource",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTimeToLive",
"dynamodb>ListTables",
"dynamodb>ListTagsOfResource",
"ec2:Describe*",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeDhcpOptions",
"ec2:DescribeFleets",
"ec2:DescribeNetworkAcls",
"ec2:DescribePlacementGroups",
"ec2:DescribeRouteTables",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeTags",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
```

```
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetInstanceTypesFromInstanceRequirements",
"ec2:GetIpamPoolAllocations",
"ec2:GetIpamPoolCidrs",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ecr-public:DescribeRepositories",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribePullThroughCacheRules",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRepositoryPolicy",
"ecr:ListTagsForResource",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:DescribeTaskSets",
"ecs:ListClusters",
"ecs:ListServices",
"ecs:ListTagsForResource",
"ecs:ListTaskDefinitionFamilies",
"ecs:ListTaskDefinitions",
"eks:DescribeAddon",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeIdentityProviderConfig",
"eks:DescribeNodegroup",
"eks:ListAddons",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListIdentityProviderConfigs",
"eks:ListNodegroups",
"eks:ListTagsForResource",
"elasticache:DescribeCacheClusters",
```

```
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheParameters",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticache:ListTagsForResource",
"elasticbeanstalk:DescribeConfigurationSettings",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticloadbalancing:DescribeListenerCertificates",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroupAttributes",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:DescribeSecurityConfiguration",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:DescribeStudio",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:GetStudioSessionMapping",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstanceFleets",
"elasticmapreduce:ListInstanceGroups",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elasticmapreduce:ListSteps",
"elasticmapreduce:ListStudios",
"elasticmapreduce:ListStudioSessionMappings",
```



```
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"es:DescribeDomain",
"es:DescribeDomains",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:GetCompatibleElasticsearchVersions",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListTags",
"events:DescribeApiDestination",
"events:DescribeArchive",
"events:DescribeConnection",
"events:DescribeEndpoint",
"events:DescribeEventBus",
"events:DescribeRule",
"events:ListApiDestinations",
"events:ListArchives",
"events:ListConnections",
"events:ListEndpoints",
"events:ListEventBuses",
"events:ListRules",
"events:ListTagsForResource",
"events:ListTargetsByRule",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"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/*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAccountActivityAccess

説明：ユーザーがアカウントアクティビティページにアクセスできるようにします。

AWSAccountActivityAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountActivityAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2023 年 3 月 7 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAccountManagementFullAccess

説明：AWS アカウント管理へのフルアクセスを提供します。

AWSAccountManagementFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountManagementFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 30 日 23:20 UTC
- 編集日時: 2021 年 9 月 30 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAccountManagementReadOnlyAccess

説明： AWS アカウント管理への読み取り専用アクセスを提供します

AWSAccountManagementReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountManagementReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 9 月 30 日 23:29 UTC
- 編集日時: 2021 年 9 月 30 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAccountUsageReportAccess

説明：ユーザーがアカウント使用状況レポートページにアクセスできるようにします。

AWSAccountUsageReportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAccountUsageReportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAgentlessDiscoveryService

説明： Discovery Agentless Connector が AWS Application Discovery Service に登録するためのアクセスを提供します。

AWSAgentlessDiscoveryService は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAgentlessDiscoveryService をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 8 月 2 日 01:35 UTC
- 編集日時: 2020 年 2 月 24 日 23:08 UTC

- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppFabricFullAccess

説明: AWS AppFabric サービスへのフルアクセスと、S3、Kinesis、KMS などの依存サービスへの読み取り専用アクセスを提供します。

AWSAppFabricFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppFabricFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 19:51 UTC
- 編集日時: 2023 年 6 月 27 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppFabricReadOnlyAccess

説明： への読み取り専用アクセスを提供します AWS AppFabric

AWSAppFabricReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppFabricReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 19:52 UTC
- 編集日時: 2023 年 6 月 27 日 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppFabricServiceRolePolicy

説明: ユーザーに代わって AWS リソース AppFabric へのアクセスを提供します

AWSAppFabricServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 26 日 21:07 UTC
- 編集日時: 2023 年 6 月 26 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

説明： Application Auto Scaling に AppStream および へのアクセス許可を付与するポリシー CloudWatch。

AWSApplicationAutoscalingAppStreamFleetPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 19:04 UTC
- 編集日時: 2017 年 10 月 20 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingCassandraTablePolicy

説明 : Application Auto Scaling に Cassandra と へのアクセス許可を付与するポリシー CloudWatch。

AWSApplicationAutoscalingCassandraTablePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 3 月 18 日 22:49 UTC
- 編集日時: 2020 年 3 月 18 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

説明： Comprehend と にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingComprehendEndpointPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 14 日 18:39 UTC
- 編集日時: 2019 年 11 月 14 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
        "*"
    ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoScalingCustomResourcePolicy

説明： APIGateway にアクセスするためのアクセス許可とカスタムリソーススケーリング CloudWatch のためのアクセス許可を Application Auto Scaling に付与するポリシー

AWSApplicationAutoScalingCustomResourcePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 4 日 23:22 UTC
- 編集日時: 2018 年 6 月 4 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

説明: Application Auto Scaling に DynamoDB と へのアクセス許可を付与するポリシー CloudWatch。

AWSApplicationAutoscalingDynamoDBTablePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 20 日 21:34 UTC
- 編集日時: 2017 年 10 月 20 日 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

説明： EC2 スポットフリート および にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 18:23 UTC
- 編集日時: 2017 年 10 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingECSServicePolicy

説明： EC2 Container Service および にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingECSServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 25 日 23:53 UTC
- 編集日時: 2017 年 10 月 25 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

説明: Amazon ElastiCache および Amazon にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingElastiCacheRGPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 23:41 UTC
- 編集日時: 2021 年 8 月 17 日 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

説明 : Application Auto Scaling に Elastic Map Reduce と にアクセスするためのアクセス許可を付与するポリシー CloudWatch。

AWSApplicationAutoscalingEMRInstanceGroupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 26 日 00:57 UTC
- 編集日時: 2017 年 10 月 26 日 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingKafkaClusterPolicy

説明： Apache Kafka および の Managed Streaming にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingKafkaClusterPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 24 日 18:36 UTC
- 編集日時: 2020 年 8 月 24 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

説明: Lambda と にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingLambdaConcurrencyPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 21 日 20:04 UTC
- 編集日時: 2019 年 10 月 21 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

説明： Amazon Neptune と Amazon にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingNeptuneClusterPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 2 日 21:14 UTC
- 編集日時: 2021 年 9 月 2 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingRDSClusterPolicy

説明: RDS と にアクセスするためのアクセス許可を Application Auto Scaling に付与するポリシー CloudWatch。

AWSApplicationAutoscalingRDSClusterPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 17 日 17:46 UTC

- 編集日時: 2018 年 8 月 7 日 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSApplicationAutoscalingRDSClusterPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

説明： Application Auto Scaling に SageMaker および へのアクセス許可を付与するポリシー CloudWatch。

AWSApplicationAutoscalingSageMakerEndpointPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 6 日 19:58 UTC
- 編集日時: 2023 年 11 月 13 日 18:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationDiscoveryAgentAccess

説明： Discovery Agent が AWS Application Discovery Service に登録するためのアクセスを提供します。

AWSApplicationDiscoveryAgentAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryAgentAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 5 月 11 日 21:38 UTC
- 編集日時: 2020 年 2 月 24 日 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "arsenal:RegisterOnPremisesAgent"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "mgh:GetHomeRegion"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

説明 : Application Discovery Service エージェントレスコレクターが Application Discovery Service を自動的に更新、登録、および通信することを許可する

AWSApplicationDiscoveryAgentlessCollectorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryAgentlessCollectorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 16 日 21:00 UTC
- 編集日時: 2022 年 8 月 16 日 21:00 UTC

- ARN: arn:aws:iam::aws:policy/
AWSApplicationDiscoveryAgentlessCollectorAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "sts:GetServiceBearerToken"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationDiscoveryServiceFullAccess

説明： AWS Application Discovery Service によって管理される設定項目を表示およびタグ付けするためのフルアクセスを提供します

AWSApplicationDiscoveryServiceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationDiscoveryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 5 月 11 日 21:30 UTC
- 編集日時: 2019 年 6 月 19 日 21:21 UTC

- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationAgentInstallationPolicy

説明：このポリシーでは、AWS アプリケーション移行サービス (MGN) AWS で外部サーバーをに
移行するために使用するレプリケーションエージェントをインストールできます AWS。このポリ
シーを、レプリケーションエージェントのインストール時に指定した認証情報を持つ AWS IAM ユー
ザーまたはロールにアタッチします。

AWSApplicationMigrationAgentInstallationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentInstallationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 6 月 19 日 07:51 UTC
- 編集日時: 2022 年 9 月 20 日 11:21 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationAgentInstallationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationAgentPolicy

説明：このポリシーでは、AWS アプリケーション移行サービス (MGN) AWS で外部サーバーをに 移行するために使用するレプリケーションエージェントをインストールして使用できます AWS。このポリシーを、レプリケーションエージェントのインストール時に指定した認証情報を持つ AWS IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationAgentPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:00 UTC
- 編集日時: 2022 年 9 月 20 日 11:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationAgentPolicy_v2

説明：このポリシーでは、AWS アプリケーション移行サービス (MGN) で使用される AWS レプリケーションエージェントを使用して、外部サーバーを に移行できます AWS。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSApplicationMigrationAgentPolicy_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationAgentPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 6 月 6 日 14:14 UTC

- 編集日時: 2022 年 6 月 6 日 14:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationConversionServerPolicy

説明：このポリシーは、Application Migration Service によって起動される EC2 インスタンスである Application Migration Service (MGN) Conversion Server が MGN サービスと通信することを許可します。このポリシーの付いた IAM ロールは MGN によって (EC2 インスタンスプロファイルとして) MGN 変換サーバーにアタッチされ、MGN は必要に応じて自動的に起動および終了します。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。MGN 変換サーバーは、ユーザーが MGN コンソール、CLI、または API を使用してテストインスタンスまたはカットオーバーインスタンスを起動することを選択したときに、アプリケーション移行サービスによって使用されます。

AWSApplicationMigrationConversionServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:48 UTC
- 編集日時: 2021 年 4 月 7 日 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationEC2Access

説明：このポリシーは、Application Migration Service (MGN) を使用して移行されたサーバーを Amazon EC2 EC2 オペレーションを提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationEC2Access は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:05 UTC
- 編集日時: 2023 年 2 月 6 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationFullAccess

説明：このポリシーは、AWS Application Migration Service (MGN) のすべてのパブリック APIs に対するアクセス許可と、KMS キー情報を読み取るアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 06:56 UTC
- 編集日時: 2024 年 5 月 19 日 08:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
```



```
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
    ],
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor3",
    "Effect" : "Allow",
    "Action" : "license-manager:ListLicenseConfigurations",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor4",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor5",
    "Effect" : "Allow",
    "Action" : "iam:ListInstanceProfiles",
    "Resource" : "*"
},
{
    "Sid" : "VisualEditor6",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
    ],
    "Condition" : {
        "StringEquals" : {
            "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
},
{
```

```
"Sid" : "VisualEditor7",
"Effect" : "Allow",
"Action" : [
  "drs:DescribeSourceServers"
],
"Resource" : "*"
},
{
  "Sid" : "VisualEditor8",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    },
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
    }
  }
},
{
  "Sid" : "VisualEditor9",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListCommandInvocations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "VisualEditor10",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "VisualEditor11",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
    "arn:aws:ssm:*:*:document/AWSMigration-*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "VisualEditor12",
  "Effect" : "Allow",
  "Action" : [
    "drs:DisconnectSourceServer"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    },
    "Null" : {
      "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
    }
  }
},
{
  "Sid" : "VisualEditor13",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter",
    "ssm:PutParameter"
  ],
```

```
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
  },
  {
    "Sid" : "VisualEditor14",
    "Effect" : "Allow",
    "Action" : [
      "servicequotas:GetServiceQuota"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "VisualEditor15",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
  },
  {
    "Sid" : "VisualEditor16",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetDocument"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
      "arn:aws:ssm:*:*:document/AWSMigration-*"
    ]
  },
  {
    "Sid" : "VisualEditor17",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
},
```

```
{
  "Sid" : "VisualEditor18",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartAutomationExecution"
  ],
  "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "mgn.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor19",
  "Effect" : "Allow",
  "Action" : "ssm:ListCommands",
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "ssm.amazonaws.com"
    }
  }
},
{
  "Sid" : "VisualEditor20",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeParameters"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "mgn.amazonaws.com"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationMGHAccess

説明：このポリシーにより、AWS Application Migration Service (MGN) は、MGN を使用して Migration AWS Hub (MGH) に移行されるサーバーの進行状況に関するメタデータを送信できます。MGN は、このポリシーがアタッチされた IAM ロールを自動的に作成し、このロールを引き受けます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSApplicationMigrationMGHAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationMGHAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:10 UTC
- 編集日時: 2021 年 4 月 7 日 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationReadOnlyAccess

説明：このポリシーは、Application Migration Service (MGN) のすべての読み取り専用パブリック APIs と、MGN コンソールの読み取り専用使用を完全にするために必要な他の AWS サービスの一部の読み取り専用 APIs へのアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSApplicationMigrationReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 7 日 07:15 UTC
- 編集日時: 2023 年 3 月 20 日 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationReplicationServerPolicy

説明：このポリシーは、Application Migration Service (MGN) レプリケーションサーバーを許可します。これは、Application Migration Service によって起動される EC2 インスタンスであり、MGN サービスと通信し、で EBS スナップショットを作成します AWS アカウント。このポリシーを含む IAM ロールは、アプリケーション移行サービスによって MGN レプリケーションサーバーに (EC2 イ

インスタンスプロファイルとして) アタッチされます。MGN レプリケーションサーバーは、必要に応じて MGN によって自動的に起動および終了されます。MGN レプリケーションサーバーは、MGN を使用して管理される移行プロセスの一環として AWS、外部サーバーからへのデータレプリケーションを容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSApplicationMigrationReplicationServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationReplicationServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 4 月 7 日 07:21 UTC
- 編集日時: 2021 年 4 月 7 日 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationServiceEc2InstancePolicy

説明: このポリシーでは、AWS アプリケーション移行サービス (AWS MGN) AWS が EC2 (クロスリージョンまたはクロス AZ) で実行されるソースサーバーを移行するために使用するレプリケーションエージェントをインストールして使用できます。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

AWSApplicationMigrationServiceEc2InstancePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationServiceEc2InstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 8 月 22 日 13:19 UTC
- 編集日時: 2024 年 1 月 3 日 14:19 UTC
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationServiceEc2InstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationServiceRolePolicy

説明：AWS アプリケーション移行サービスがユーザーに代わって AWS リソースを作成および管理できるようにします。

AWSApplicationMigrationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 7 日 06:43 UTC
- 編集日時: 2023 年 6 月 20 日 09:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:DescribeInstanceState",
    "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"
      ]
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationSSMAccess

説明：このポリシーは、Application Migration Service (MGN) を使用して移行後のカスタムコマンド SSM ドキュメントを実行するために必要な Amazon SSM オペレーションへのアクセスを提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationSSMAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationSSMAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 11 月 27 日 9:29 UTC
- 編集日時: 2023 年 3 月 20 日 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSApplicationMigrationVCenterClientPolicy

説明：このポリシーでは、外部サーバーを に移行するために AWS Application Migration Service (MGN) で使用される AWS VCenter Client をインストールして使用することを許可します AWS。このポリシーを AWS VCenter Client のインストール時に認証情報を提供する IAM ユーザーまたはロールにアタッチします。

AWSApplicationMigrationVCenterClientPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSApplicationMigrationVCenterClientPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 8 日 12:53 UTC
- 編集日時: 2021 年 11 月 8 日 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshEnvoyAccess

説明： 仮想ノード設定にアクセスするための App Mesh Envoy ポリシー。

AWSAppMeshEnvoyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 3 日 21:29 UTC
- 編集日時: 2019 年 7 月 3 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshFullAccess

説明： AWS App Mesh APIsとマネジメントコンソールへのフルアクセスを提供します。

AWSAppMeshFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 16 日 17:50 UTC
- 編集日時: 2021 年 1 月 7 日 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshPreviewEnvoyAccess

説明： 仮想ノード設定にアクセスするための App Mesh Preview Envoy ポリシー。

AWSAppMeshPreviewEnvoyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshPreviewEnvoyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 8 月 5 日 23:32 UTC
- 編集日時: 2019 年 8 月 5 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshPreviewServiceRolePolicy

説明： AWS App Mesh が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AWSAppMeshPreviewServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 19 日 19:07 UTC
- 編集日時: 2019 年 8 月 21 日 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```


詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshReadOnly

説明： AWS App Mesh APIsとマネジメントコンソールへの読み取り専用アクセスを提供します。

AWSAppMeshReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppMeshReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 16 日 17:51 UTC
- 編集日時: 2021 年 1 月 7 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppMeshServiceRolePolicy

説明 : が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする AWS AppMesh

AWSAppMeshServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 3 日 18:30 UTC
- 編集日時: 2023 年 10 月 10 日 16:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ACMCertificateVerification",
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppRunnerFullAccess

説明: すべての App Runner アクションにアクセス許可を付与します。

AWSAppRunnerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 1 月 11 日 04:02 UTC
- 編集日時: 2022 年 1 月 11 日 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppRunnerReadOnlyAccess

説明 : App Runner リソースの詳細を一覧表示および表示するアクセス許可を付与します。

AWSAppRunnerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 24 日 21:24 UTC
- 編集日時: 2022 年 2 月 24 日 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Action" : [
      "apprunner:List*",
      "apprunner:Describe*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppRunnerServicePolicyForECRAccess

説明：お客様のアカウントの Amazon ECR リソースに読み取りアクセス許可を付与する AWS App Runner サービスポリシー。App Runner サービスを作成または更新するときに App Runner に渡されるロールで使用してください。

AWSAppRunnerServicePolicyForECRAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppRunnerServicePolicyForECRAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 5 月 14 日 19:17 UTC
- 編集日時: 2021 年 5 月 14 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppSyncAdministrator

説明： AppSync サービスへの管理アクセスを提供しますが、コンソール経由で にアクセスするのに十分ではありません。

AWSAppSyncAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:20 UTC
- 編集日時: 2019 年 11 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppSyncInvokeFullAccess

説明：コンソール経由および個別に、AppSync サービスへの完全な呼び出しアクセスを提供します

AWSAppSyncInvokeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncInvokeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2018 年 3 月 20 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAppSyncPushToCloudWatchLogs

説明 : AppSync がユーザーの CloudWatch アカウントにログをプッシュできるようにします。

AWSAppSyncPushToCloudWatchLogs は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncPushToCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 9 日 19:38 UTC
- 編集日時: 2018 年 4 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppSyncSchemaAuthor

説明：スキーマを作成、更新、クエリするためのアクセスを提供します。

AWSAppSyncSchemaAuthor は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAppSyncSchemaAuthor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 20 日 21:21 UTC
- 編集日時: 2023 年 2 月 1 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAppSyncServiceRolePolicy

説明：が使用または管理する AWS サービスとリソースへのアクセスを有効にする AppSync

AWSAppSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 1 月 21 日 19:56 UTC
- 編集日時: 2020 年 1 月 21 日 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSArtifactAccountSync

説明： AWS アーティファクトに AWS Organizations のオペレーションへの読み取り専用アクセスを許可します。

AWSArtifactAccountSync は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactAccountSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 4 月 10 日 23:04 UTC
- 編集日時: 2018 年 4 月 10 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSArtifactReportsReadOnlyAccess

説明： AWS Artifact サービスレポートへの読み取り専用アクセスを提供します。

AWSArtifactReportsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSArtifactReportsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 1 月 2 日 22:42 UTC
- 編集日時: 2024 年 1 月 2 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ]
    }
  ]
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSArtifactServiceRolePolicy

説明： AWS Artifact が AWS Organizations サービスを介して組織に関する情報を収集できるようにします。

AWSArtifactServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 8 月 21 日 20:27 UTC
- 編集日時: 2023 年 8 月 21 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAuditManagerAdministratorAccess

説明： AWS Audit Manager の有効化または無効化、設定の更新、評価、コントロール、フレームワークの管理を行うための管理アクセスを提供します

AWSAuditManagerAdministratorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSAuditManagerAdministratorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 11 日 20:02 UTC
- 編集日時: 2024 年 5 月 15 日 23:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
    },
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "AllowOnlyAuditManagerIntegration",
    "Effect" : "Allow",
    "Action" : [
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator",
      "organizations:EnableAWSServiceAccess"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "organizations:ServicePrincipal" : [
          "auditmanager.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "IAMAccess",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetUser",
      "iam:ListUsers",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "IAMAccessCreateSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "auditmanager.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "IAMAccessManageSLR",
    "Effect" : "Allow",
```

```
    "Action" : [
      "iam:DeleteServiceLinkedRole",
      "iam:UpdateRoleDescription",
      "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
  },
  {
    "Sid" : "S3Access",
    "Effect" : "Allow",
    "Action" : [
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : "true"
      },
      "StringLike" : {
        "kms:ViaService" : "auditmanager.*.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SNSAccess",
```

```
    "Effect" : "Allow",
    "Action" : [
      "sns:ListTopics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateEventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "events:PutRule"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "events:detail-type" : "Security Hub Findings - Imported"
      },
      "ForAllValues:StringEquals" : {
        "events:source" : [
          "aws.securityhub"
        ]
      }
    }
  },
  {
    "Sid" : "EventsAccess",
    "Effect" : "Allow",
    "Action" : [
      "events>DeleteRule",
      "events:DescribeRule",
      "events:EnableRule",
      "events:DisableRule",
      "events:ListTargetsByRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  },
  {
    "Sid" : "TagAccess",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
  },
```



```
    "Resource" : "*"
  },
  {
    "Sid" : "ControlCatalogAccess",
    "Effect" : "Allow",
    "Action" : [
      "controlcatalog:ListCommonControls",
      "controlcatalog:ListDomains",
      "controlcatalog:ListObjectives"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSAuditManagerServiceRolePolicy

説明： AWS Audit Manager が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

AWSAuditManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 8 日 15:12 UTC

- 編集日時：2024 年 6 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
```

```
"cloudwatch:GetMetricStatistics",
"cloudwatch:ListMetrics",
"cognito-idp:DescribeUserPool",
"config:DescribeConfigRules",
"config:DescribeDeliveryChannels",
"config:ListDiscoveredResources",
"directconnect:DescribeDirectConnectGateways",
"directconnect:DescribeVirtualGateways",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeBackup",
"dynamodb:DescribeTableReplicaAutoScaling",
"dynamodb:DescribeTable",
"dynamodb:ListBackups",
"dynamodb:ListGlobalTables",
"dynamodb:ListTables",
"ec2:DescribeInstanceCreditSpecifications",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:GetLaunchTemplateData",
"ec2:DescribeAddresses",
"ec2:DescribeCustomerGateways",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeFlowLogs",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGateways",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeTransitGateways",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetEbsEncryptionByDefault",
```

```
"ecs:DescribeClusters",
"eks:DescribeAddonVersions",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeServiceUpdates",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeSslPolicies",
"elasticloadbalancing:DescribeTargetGroups",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListSecurityConfigurations",
"events:DescribeRule",
"events:ListConnections",
"events:ListEventBuses",
"events:ListEventSources",
"events:ListRules",
"firehose:ListDeliveryStreams",
"fsx:DescribeFileSystems",
"guardduty:ListDetectors",
"iam:GenerateCredentialReport",
"iam:GetAccountAuthorizationDetails",
"iam:GetAccessKeyLastUsed",
"iam:GetCredentialReport",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:ListAttachedGroupPolicies",
"iam:ListAttachedUserPolicies",
"iam:ListEntitiesForPolicy",
"iam:ListGroupsForUser",
"iam:ListGroupPolicies",
"iam:ListGroups",
"iam:ListOpenIdConnectProviders",
"iam:ListPolicies",
"iam:ListRolePolicies",
"iam:ListRoles",
"iam:ListSamlProviders",
"iam:ListUserPolicies",
"iam:ListUsers",
```

```
"iam:ListVirtualMFADevices",
"iam:ListPolicyVersions",
"iam:ListAccessKeys",
"iam:ListAttachedRolePolicies",
"iam:ListMfaDeviceTags",
"iam:ListMfaDevices",
"kafka:ListClusters",
"kafka:ListKafkaVersions",
"kinesis:ListStreams",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:GetKeyRotationStatus",
"kms:ListGrants",
"kms:ListKeyPolicies",
"kms:ListKeys",
"lambda:ListFunctions",
"license-manager:ListAssociationsForLicenseConfiguration",
"license-manager:ListLicenseConfigurations",
"license-manager:ListUsageForLicenseConfiguration",
"logs:DescribeDestinations",
"logs:DescribeExportTasks",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"logs:DescribeResourcePolicies",
"logs:FilterLogEvents",
"logs:GetDataProtectionPolicy",
"es:DescribeDomains",
"es:DescribeDomain",
"es:DescribeDomainConfig",
"es:ListDomainNames",
"organizations:DescribeOrganization",
"organizations:DescribePolicy",
"rds:DescribeCertificates",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeLoggingStatus",
"route53:GetQueryLoggingConfig",
"sagemaker:DescribeAlgorithm",
```

```
"sagemaker:DescribeFlowDefinition",
"sagemaker:DescribeHumanTaskUi",
"sagemaker:DescribeModelBiasJobDefinition",
"sagemaker:DescribeModelCard",
"sagemaker:DescribeModelQualityJobDefinition",
"sagemaker:DescribeDomain",
"sagemaker:DescribeEndpoint",
"sagemaker:DescribeEndpointConfig",
"sagemaker:DescribeLabelingJob",
"sagemaker:DescribeModel",
"sagemaker:DescribeTrainingJob",
"sagemaker:DescribeUserProfile",
"sagemaker:ListAlgorithms",
"sagemaker:ListDomains",
"sagemaker:ListEndpoints",
"sagemaker:ListEndpointConfigs",
"sagemaker:ListFlowDefinitions",
"sagemaker:ListHumanTaskUis",
"sagemaker:ListLabelingJobs",
"sagemaker:ListModels",
"sagemaker:ListModelBiasJobDefinitions",
"sagemaker:ListModelCards",
"sagemaker:ListModelQualityJobDefinitions",
"sagemaker:ListMonitoringAlerts",
"sagemaker:ListMonitoringSchedules",
"sagemaker:ListTrainingJobs",
"sagemaker:ListUserProfiles",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketVersioning",
"s3:GetEncryptionConfiguration",
"s3:GetLifecycleConfiguration",
"s3:ListAllMyBuckets",
"secretsmanager:DescribeSecret",
"secretsmanager:ListSecrets",
"securityhub:DescribeStandards",
"sns:ListTagsForResource",
"sns:ListTopics",
"sqs:ListQueues",
"waf-regional:GetRule",
"waf-regional:GetWebAcl",
"waf:GetRule",
"waf:GetRuleGroup",
"waf:ListActivatedRulesInRuleGroup",
"waf:ListWebAcls",
```

```
    "wafv2:ListWebAcls",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf-regional:ListRules",
    "waf:ListRuleGroups",
    "waf:ListRules"
  ],
  "Resource" : "*",
  "Sid" : "APIsAccess"
},
{
  "Sid" : "S3Access",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketAcl",
    "s3:GetBucketLogging",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketTagging"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : [
        "${aws:PrincipalAccount}"
      ]
    }
  }
},
{
  "Sid" : "APIGatewayAccess",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/restapis/*/stages"
  ],
  "Condition" : {
    "StringEquals" : {
```

```
    "aws:ResourceAccount" : [
      "${aws:PrincipalAccount}"
    ]
  }
}
},
{
  "Sid" : "CreateEventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:PutRule"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
  "Condition" : {
    "StringEquals" : {
      "events:detail-type" : "Security Hub Findings - Imported"
    },
    "Null" : {
      "events:source" : "false"
    },
    "ForAllValues:StringEquals" : {
      "events:source" : [
        "aws.securityhub"
      ]
    }
  }
},
{
  "Sid" : "EventsAccess",
  "Effect" : "Allow",
  "Action" : [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
}
]
```


詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

説明： AWS Auto Scaling に、定期的にキャパシティを予測し、スケーリングプラン内の Auto Scaling グループのスケジュールされたスケーリングアクションを生成するアクセス許可を付与するポリシー

AWSAutoScalingPlansEC2AutoScalingPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 23 日 22:46 UTC
- 編集日時: 2018 年 8 月 23 日 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupAuditAccess

説明: このポリシーは、AWS バックアップリソースとアクティビティに対する期待を定義するコントロールとフレームワークを作成し、定義されたコントロールとフレームワークに対して AWS バックアップリソースとアクティビティを監査するアクセス許可をユーザーに付与します。このポリシーは、AWS Config および同様のサービスにアクセス許可を付与して、監査を実行するユーザーの期待を記述します。このポリシーは、S3 および同様のサービスに監査レポートを配信するアクセス権限も付与し、ユーザーは監査レポートを見つけて開くことができます。

AWSBackupAuditAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupAuditAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 8 月 24 日 01:02 UTC
- 編集日時: 2023 年 4 月 10 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupDataTransferAccess

説明：このポリシーでは、AWS Backint エージェントは AWS Backup Storage プレーンを使用してバックアップデータ転送を完了できます。このポリシーを Backint エージェントで SAP HANA を実行している EC2 インスタンスが引き受けるロールにアタッチします。

AWSBackupDataTransferAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupDataTransferAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 22:48 UTC
- 編集日時: 2022 年 11 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupFullAccess

説明: このポリシーはバックアップ管理者を対象としており、AWS バックアッププランの作成または編集、バックアッププランへの AWS リソースの割り当て、バックアップの削除、バックアップの復元など、バックアップオペレーションへのフルアクセスを許可します。

AWSBackupFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 18 日 22:21 UTC
- 編集日時: 2023 年 11 月 27 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

説明: ユーザーに代わって仮想マシンのメタデータを同期する AWS BackupGateway アクセス許可を付与します

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 12 月 15 日 19:43 UTC
- 編集日時: 2022 年 12 月 15 日 19:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupOperatorAccess

説明：このポリシーは、バックアッププランへの AWS リソースの割り当て、オンデマンドバックアップの作成、バックアップの復元を行うアクセス許可をユーザーに付与します。このポリシーは、ユーザーがバックアッププランを作成、または編集したり、スケジュールされたバックアップを作成後に削除したりするためのアクセス許可は持っていません。

AWSBackupOperatorAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOperatorAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2019 年 11 月 18 日 22:23 UTC
- 編集日時: 2023 年 9 月 6 日 20:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupOrganizationAdminAccess

説明：このポリシーは、クロスアカウントバックアップ管理を使用して組織のバックアップを管理するバックアップ管理者を対象としています。

AWSBackupOrganizationAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupOrganizationAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 24 日 16:23 UTC
- 編集日時: 2022 年 11 月 18 日 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupRestoreAccessForSAPHANA

説明： Amazon EC2 で SAP HANA のバックアップを復元する Backup アクセス AWS 許可を付与します

AWSBackupRestoreAccessForSAPHANA は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupRestoreAccessForSAPHANA をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 10 日 22:43 UTC
- 編集日時: 2022 年 11 月 10 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceLinkedRolePolicyForBackup

説明：AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

AWSBackupServiceLinkedRolePolicyForBackup は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 2 日 23:08 UTC
- 編集日時: 2024 年 5 月 17 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup

ポリシーのバージョン

ポリシーのバージョン: v16 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "DescribePermissions",
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources",
    "elasticfilesystem:DescribeFileSystems",
    "dynamodb:ListTables",
    "storagegateway:ListVolumes",
    "ec2:DescribeVolumes",
    "ec2:DescribeInstances",
    "rds:DescribeDBInstances",
    "rds:DescribeDBClusters",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SnapshotCopyTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*::snapshot/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CopySnapshot"
    }
  }
},
{
  "Sid" : "EC2CreateBackupTagPermissions",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*::image/*",
    "arn:aws:ec2:*::snapshot/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
```



```
        "AWSBackupManagedResource"
      ]
    }
  },
  {
    "Sid" : "EC2CreateTagsPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*::image/*",
      "arn:aws:ec2:*::snapshot/*"
    ],
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AWSBackupManagedResource" : "false"
      }
    }
  },
  {
    "Sid" : "EC2RDSDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeSnapshots",
      "ec2:DescribeSnapshotTierStatus",
      "ec2:DescribeImages",
      "rds:DescribeDBSnapshots",
      "rds:DescribeDBClusterSnapshots"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EBSCopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopySnapshot",
    "Resource" : "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Sid" : "EC2CopyPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:CopyImage",
    "Resource" : "*"
  },
  {
```

```
"Sid" : "EC2ModifyPermissions",
"Effect" : "Allow",
"Action" : [
  "ec2:DeregisterImage",
  "ec2:DeleteSnapshot",
  "ec2:ModifySnapshotTier"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "ec2:ResourceTag/AWSBackupManagedResource" : "false"
  }
}
},
{
  "Sid" : "RDSInstanceAndSnapshotPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:CopyDBSnapshot",
    "rds>DeleteDBSnapshot",
    "rds>DeleteDBInstanceAutomatedBackup"
  ],
  "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
},
{
  "Sid" : "RDSClusterPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rds:AddTagsToResource",
    "rds:CopyDBClusterSnapshot",
    "rds>DeleteDBClusterSnapshot"
  ],
  "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
},
{
  "Sid" : "KMSDescribePermissions",
  "Effect" : "Allow",
  "Action" : "kms:DescribeKey",
  "Resource" : "*"
},
{
  "Sid" : "KMSGrantPermissions",
  "Effect" : "Allow",
```

```
"Action" : [
  "kms:ListGrants",
  "kms:ReEncryptFrom",
  "kms:GenerateDataKeyWithoutPlaintext"
],
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "kms:ViaService" : [
      "ec2.*.amazonaws.com",
      "rds.*.amazonaws.com",
      "fsx.*.amazonaws.com"
    ]
  }
}
},
{
  "Sid" : "KMSCreateGrantPermissions",
  "Effect" : "Allow",
  "Action" : "kms:CreateGrant",
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : [
        "ec2.*.amazonaws.com",
        "rds.*.amazonaws.com",
        "fsx.*.amazonaws.com"
      ]
    }
  }
}
},
{
  "Sid" : "FsxPermissions",
  "Effect" : "Allow",
  "Action" : [
    "fsx:CopyBackup",
    "fsx:TagResource",
    "fsx:DescribeBackups",
    "fsx>DeleteBackup"
  ],
  "Resource" : "arn:aws:fsx:*:*:backup/*"
```

```
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
```

```
"Action" : [
  "events:DeleteRule",
  "events:PutTargets",
  "events:DescribeRule",
  "events:EnableRule",
  "events:PutRule",
  "events:RemoveTargets",
  "events:ListTargetsByRule",
  "events:DisableRule"
],
"Resource" : [
  "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
]
},
{
  "Sid" : "EventBridgeRulesPermissions",
  "Effect" : "Allow",
  "Action" : "events:ListRules",
  "Resource" : "*"
},
{
  "Sid" : "SSMSAPPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ssm-sap:GetOperation",
    "ssm-sap:UpdateHANABackupSettings"
  ],
  "Resource" : "*"
},
{
  "Sid" : "TimestreamResourcePermissions",
  "Effect" : "Allow",
  "Action" : [
    "timestream:ListDatabases",
    "timestream:ListTables",
    "timestream:ListTagsForResource",
    "timestream:DescribeDatabase",
    "timestream:DescribeTable",
    "timestream:GetAwsBackupStatus",
    "timestream:GetAwsRestoreStatus"
  ],
  "Resource" : [
    "arn:aws:timestream:*:*:database/*"
  ]
}
```

```
  },
  {
    "Sid" : "TimestreamPermissions",
    "Effect" : "Allow",
    "Action" : [
      "timestream:DescribeEndpoints"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "RedshiftDescribePermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusterSnapshots",
      "redshift:DescribeTags"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:snapshot:*/**",
      "arn:aws:redshift:*:*:cluster:*"
    ]
  },
  {
    "Sid" : "RedshiftClusterSnapshotPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift>DeleteClusterSnapshot"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:snapshot:*/**"
    ]
  },
  {
    "Sid" : "RedshiftClusterPermissions",
    "Effect" : "Allow",
    "Action" : [
      "redshift:DescribeClusters"
    ],
    "Resource" : [
      "arn:aws:redshift:*:*:cluster:*"
    ]
  },
  {
    "Sid" : "CloudformationStackPermissions",
    "Effect" : "Allow",
```

```
    "Action" : [
      "cloudformation:ListStacks"
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/*"
    ]
  },
  {
    "Sid" : "RecoveryPointTaggingPermissions",
    "Effect" : "Allow",
    "Action" : [
      "backup:TagResource"
    ],
    "Resource" : "arn:aws:backup:*:*:recovery-point:*",
    "Condition" : {
      "StringEquals" : {
        "aws:PrincipalAccount" : "${aws:ResourceAccount}"
      }
    }
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

説明：AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

AWSBackupServiceLinkedRolePolicyForBackupTest は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 5 月 12 日 17:37 UTC
- 編集日時: 2020 年 5 月 12 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
    }  
  ]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceRolePolicyForBackup

説明： AWS サービス間でユーザーに代わってバックアップを作成する AWS Backup アクセス許可を付与します

AWSBackupServiceRolePolicyForBackup は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForBackup をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 10 日 21:01 UTC
- 編集日時: 2024 年 5 月 17 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup

ポリシーのバージョン

ポリシーのバージョン: v19 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
},
{
  "Sid" : "RecoveryPointTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:TagResource"
  ],
  "Resource" : "arn:aws:backup:*:*:recovery-point:*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceRolePolicyForRestores

説明：AWS サービス間でユーザーに代わって復元を実行するための AWS Backup アクセス許可を提供します。このポリシーには、復元プロセスの一部である EBS ボリューム、RDS EFS インスタンス、EFS ファイルシステムなどの AWS リソースを作成および削除するアクセス許可が含まれています。

AWSBackupServiceRolePolicyForRestores は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForRestores をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 12 日 00:23 UTC
- 編集日時: 2023 年 12 月 15 日 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

ポリシーのバージョン

ポリシーのバージョン: v20 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceRolePolicyForS3Backup

説明: Backup が任意の S3 バケット内のデータをバックアップするために必要なアクセス許可を含むポリシー。AWS には、すべての S3 オブジェクトへの読み取りアクセスと、すべての KMS キーに対する復号化アクセスが含まれます。

AWSBackupServiceRolePolicyForS3Backup は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForS3Backup をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 18 日 17:40 UTC
- 編集日時: 2024 年 5 月 17 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
```



```
"Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
"Effect" : "Allow",
"Action" : [
  "events:DeleteRule",
  "events:PutTargets",
  "events:DescribeRule",
  "events:EnableRule",
  "events:PutRule",
  "events:RemoveTargets",
  "events:ListTargetsByRule",
  "events:DisableRule"
],
"Resource" : [
  "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
]
},
{
  "Sid" : "EventBridgeListRulesPermissions",
  "Effect" : "Allow",
  "Action" : "events:ListRules",
  "Resource" : "*"
},
{
  "Sid" : "KmsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "kms:ViaService" : "s3.*.amazonaws.com"
    }
  }
},
{
  "Sid" : "S3BucketPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketTagging",
    "s3:GetInventoryConfiguration",
    "s3:ListBucketVersions",
    "s3:ListBucket",
```

```
    "s3:GetBucketVersioning",
    "s3:GetBucketLocation",
    "s3:GetBucketAcl",
    "s3:PutInventoryConfiguration",
    "s3:GetBucketNotification",
    "s3:PutBucketNotification"
  ],
  "Resource" : "arn:aws:s3:::*"
},
{
  "Sid" : "S3ObjectPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObjectAcl",
    "s3:GetObject",
    "s3:GetObjectVersionTagging",
    "s3:GetObjectVersionAcl",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion"
  ],
  "Resource" : "arn:aws:s3:::*/*"
},
{
  "Sid" : "S3ListBucketPermissions",
  "Effect" : "Allow",
  "Action" : "s3:ListAllMyBuckets",
  "Resource" : "*"
},
{
  "Sid" : "RecoveryPointTaggingPermissions",
  "Effect" : "Allow",
  "Action" : [
    "backup:TagResource"
  ],
  "Resource" : "arn:aws:backup:*:*:recovery-point:*",
  "Condition" : {
    "StringEquals" : {
      "aws:PrincipalAccount" : "${aws:ResourceAccount}"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBackupServiceRolePolicyForS3Restore

説明: Backup が S3 バックアップをバケットに復元するために必要なアクセス許可を含むポリシー。AWS これには、すべての S3 バケットに対する読み取り/書き込みアクセス許可と、すべての KMS キーに対する GenerateDataKey および DescribeKey に対するアクセス許可が含まれます。

AWSBackupServiceRolePolicyForS3Restore は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBackupServiceRolePolicyForS3Restore をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 2 月 18 日 17:39 UTC
- 編集日時: 2023 年 2 月 7 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBatchFullAccess

説明： Batch AWS リソースへのフルアクセスを提供します。

AWSBatchFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 6 日 19:35 UTC
- 編集日時: 2022 年 10 月 24 日 16:09 UTC
- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBatchServiceEventTargetRole

説明 : AWS バッチジョブ送信の CloudWatch イベントターゲットを有効にするポリシー

AWSBatchServiceEventTargetRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBatchServiceEventTargetRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 2 月 28 日 22:31 UTC
- 編集日時: 2018 年 2 月 28 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBatchServiceRole

説明： EC2、Autoscaling、EC2 Container Service、Cloudwatch Logs などの関連サービスへのアクセスを許可する AWS Batch サービスロールのポリシー。

AWSBatchServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBatchServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 19:36 UTC
- 編集日時: 2023 年 12 月 5 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBCMDataExportsServiceRolePolicy

説明：請求情報とコスト管理データエクスポートに、顧客に代わって Amazon S3 などのターゲットロケーションにデータをエクスポートするための AWS サービスデータへのアクセスを提供するサービスにリンクされたロール。

AWSBCMDataExportsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 6 月 10 日 17:40 UTC
- 編集日時: 2024 年 6 月 10 日 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Effect" : "Allow",
    "Action" : [
      "cost-optimization-hub:ListEnrollmentStatuses",
      "cost-optimization-hub:ListRecommendations"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBillingConductorFullAccess

説明 : AWSBillingConductorFullAccess 管理ポリシーを使用して、AWS Billing Conductor (ABC) コンソールと APIs への完全なアクセスを許可します。このポリシーにより、ユーザーは ABC リソースを一覧表示、作成、削除できます。

AWSBillingConductorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingConductorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2022 年 4 月 13 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBillingConductorReadOnlyAccess

説明: AWSBillingConductorReadOnlyAccess 管理ポリシーを使用して、AWS Billing Conductor (ABC) コンソールと APIs への読み取り専用アクセスを許可します。このポリシーは、すべての ABC リソースを取得して一覧表示するアクセス許可を付与します。リソースを作成または削除したりする機能は含まれません。

AWSBillingConductorReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSBillingConductorReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 13 日 18:02 UTC
- 編集日時: 2022 年 4 月 13 日 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```


詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBillingReadOnlyAccess

説明：請求コンソールで請求を表示できるようにします。

AWSBillingReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBillingReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 27 日 20:08 UTC
- 編集日時: 2024 年 5 月 23 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Sid" : "VisualEditor0",
"Effect" : "Allow",
"Action" : [
  "account:GetAccountInformation",
  "aws-portal:ViewBilling",
  "billing:GetBillingData",
  "billing:GetBillingDetails",
  "billing:GetBillingNotifications",
  "billing:GetBillingPreferences",
  "billing:GetCredits",
  "billing:GetContractInformation",
  "billing:GetIAMAccessPreference",
  "billing:GetSellerOfRecord",
  "billing:ListBillingViews",
  "budgets:ViewBudget",
  "budgets:DescribeBudgetActionsForBudget",
  "budgets:DescribeBudgetAction",
  "budgets:DescribeBudgetActionsForAccount",
  "budgets:DescribeBudgetActionHistories",
  "ce:DescribeCostCategoryDefinition",
  "ce:GetCostAndUsage",
  "ce:ListCostCategoryDefinitions",
  "ce:ListTagsForResource",
  "ce:ListCostAllocationTags",
  "ce:ListCostAllocationTagBackfillHistory",
  "ce:GetTags",
  "ce:GetDimensionValues",
  "consolidatedbilling:ListLinkedAccounts",
  "consolidatedbilling:GetAccountBillingRole",
  "cur:GetClassicReport",
  "cur:GetClassicReportPreferences",
  "cur:GetUsageReport",
  "cur:DescribeReportDefinitions",
  "freetier:GetFreeTierAlertPreference",
  "freetier:GetFreeTierUsage",
  "invoicing:GetInvoiceEmailDeliveryPreferences",
  "invoicing:GetInvoicePDF",
  "invoicing:ListInvoiceSummaries",
  "payments:GetPaymentInstrument",
  "payments:GetPaymentStatus",
  "payments:ListPaymentPreferences",
  "payments:ListTagsForResource",
  "payments:ListPaymentInstruments",
  "purchase-orders:GetPurchaseOrder",
```

```
    "purchase-orders:ViewPurchaseOrders",
    "purchase-orders:ListPurchaseOrderInvoices",
    "purchase-orders:ListPurchaseOrders",
    "purchase-orders:ListTagsForResource",
    "sustainability:GetCarbonFootprintSummary",
    "tax:GetTaxRegistrationDocument",
    "tax:GetTaxInheritance",
    "tax:ListTaxRegistrations"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

説明：このポリシーは、AWS リソースを制御するアクセス許可を付与します。例えば、AWS Systems Manager (SSM) スクリプトを実行して EC2 インスタンスまたは RDS インスタンスを起動および停止するには、次のようにします。

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 5 月 25 日 19:03 UTC
- 編集日時: 2022 年 5 月 25 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBudgetsActionsWithAWSResourceControlAccess

説明： AWS Budgets Actions を使用して実行中の AWS リソースの状態を制御するなど、 Budgets Actions へのフルアクセスを 経由で提供します。 AWS Management Console

AWSBudgetsActionsWithAWSResourceControlAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsActionsWithAWSResourceControlAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 15 日 17:19 UTC
- 編集日時: 2020 年 10 月 15 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActionsWithAWSResourceControlAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBudgetsReadOnlyAccess

説明： 経由で AWS Budgets コンソールへの読み取り専用アクセスを提供します AWS Management Console。

AWSBudgetsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBudgetsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 15 日 17:18 UTC

- 編集日時: 2020 年 10 月 15 日 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSBugBustFullAccess

説明：この IAM ポリシーは、ユーザーに AWS BugBust コンソールへのフルアクセスを付与します。

AWSBugBustFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBugBustFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 6 月 24 日 07:03 UTC
- 編集日時: 2021 年 7 月 22 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBugBustPlayerAccess

説明：この IAM ポリシーは、AWS BugBust イベントに参加するアクセスをユーザーに許可します

AWSBugBustPlayerAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSBugBustPlayerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 6 月 24 日 07:15 UTC
- 編集日時: 2021 年 6 月 24 日 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSBugBustServiceRolePolicy

説明：ユーザーに代わって リソースにアクセス AWS BugBust するためのアクセス許可を に付与します

AWSBugBustServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 24 日 06:59 UTC
- 編集日時: 2021 年 6 月 24 日 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerFullAccess

説明： AWS Certificate Manager (ACM) へのフルアクセスを提供します

AWSCertificateManagerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 21 日 17:02 UTC
- 編集日時: 2020 年 8 月 17 日 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerPrivateCAAuditor

説明： AWS Certificate Manager プライベート認証機関への監査アクセスを提供する

AWSCertificateManagerPrivateCAAuditor は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAAuditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:51 UTC
- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerPrivateCAFullAccess

説明： AWS Certificate Manager プライベート認証機関へのフルアクセスを提供します

AWSCertificateManagerPrivateCAFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCertificateManagerPrivateCAFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 10 月 23 日 16:54 UTC
- 編集日時: 2018 年 10 月 23 日 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerPrivateCAPrivilegedUser

説明 : Certificate AWS Manager プライベート認証機関への特権証明書ユーザーアクセスを提供する

AWSCertificateManagerPrivateCAPrivilegedUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAPrivilegedUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 20 日 17:43 UTC
- 編集日時: 2019 年 6 月 20 日 17:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerPrivateCAReadOnly

説明： AWS Certificate Manager プライベート認証機関への読み取り専用アクセスを提供します

AWSCertificateManagerPrivateCAReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:57 UTC
- 編集日時: 2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerPrivateCAUser

説明： Certificate Manager プライベート認証機関への AWS 証明書ユーザーアクセスを提供します

AWSCertificateManagerPrivateCAUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerPrivateCAUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 23 日 16:53 UTC
- 編集日時: 2019 年 6 月 20 日 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

ポリシーのバージョニング

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCertificateManagerReadOnly

説明 : AWS Certificate Manager (ACM) への読み取り専用アクセスを提供します。

AWSCertificateManagerReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCertificateManagerReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 21 日 17:07 UTC
- 編集日時: 2021 年 3 月 15 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSChatbotServiceLinkedRolePolicy

説明 : AWS Chatbot で使用されるサービスにリンクされたロール。

AWSChatbotServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 18 日 16:39 UTC
- 編集日時: 2019 年 11 月 18 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCleanRoomsFullAccess

説明： AWS Clean Rooms リソースへのフルアクセスと、関連する へのアクセスを許可します AWS のサービス。

AWSCleanRoomsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC
- 編集日時: 2024 年 3 月 21 日 15:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCleanRoomsFullAccessNoQuerying

説明： コラボレーションでのクエリと、関連する へのアクセスを除き、AWS クリーンルームリソースへのフルアクセスを許可します AWS のサービス。

AWSCleanRoomsFullAccessNoQuerying は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsFullAccessNoQuerying をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:12 UTC
- 編集日時: 2024 年 5 月 14 日 18:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms>DeleteAnalysisTemplate",
        "cleanrooms>DeleteCollaboration",
        "cleanrooms>DeleteConfiguredTable",
        "cleanrooms>DeleteConfiguredTableAnalysisRule",
        "cleanrooms>DeleteConfiguredTableAssociation",
        "cleanrooms>DeleteMember",
        "cleanrooms>DeleteMembership",

```

```
    "cleanrooms:GetAnalysisTemplate",
    "cleanrooms:GetCollaborationAnalysisTemplate",
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetConfiguredTable",
    "cleanrooms:GetConfiguredTableAnalysisRule",
    "cleanrooms:GetConfiguredTableAssociation",
    "cleanrooms:GetMembership",
    "cleanrooms:GetProtectedQuery",
    "cleanrooms:GetSchema",
    "cleanrooms:GetSchemaAnalysisRule",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:UpdateAnalysisTemplate",
    "cleanrooms:UpdateCollaboration",
    "cleanrooms:UpdateConfiguredTable",
    "cleanrooms:UpdateConfiguredTableAnalysisRule",
    "cleanrooms:UpdateConfiguredTableAssociation",
    "cleanrooms:UpdateMembership",
    "cleanrooms:ListTagsForResource",
    "cleanrooms:UntagResource",
    "cleanrooms:TagResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CleanRoomsNoQuerying",
  "Effect" : "Deny",
  "Action" : [
    "cleanrooms:StartProtectedQuery",
    "cleanrooms:UpdateProtectedQuery"
  ],
  "Resource" : "*"
},
{
  "Sid" : "PassServiceRole",
  "Effect" : "Allow",
  "Action" : [
```

```
    "iam:PassRole"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "ListRolesToPickServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListRoles"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
  ],
  "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
},
{
  "Sid" : "ListPoliciesToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListPolicies"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetPolicyToInspectServiceRolePolicy",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
  ],
  "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
},
```

```
{
  "Sid" : "ConsoleDisplayTables",
  "Effect" : "Allow",
  "Action" : [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EstablishLogDeliveries",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs>DeleteLogDelivery",
    "logs:ListLogDeliveries"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
},
{
  "Sid" : "SetupLogGroupsDescribe",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : "cleanrooms.amazonaws.com"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "SetupLogGroupsCreate",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "SetupLogGroupsResourcePolicy",
    "Effect" : "Allow",
    "Action" : [
      "logs:DescribeResourcePolicies",
      "logs:PutResourcePolicy"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cleanrooms.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleLogSummaryQueryLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
    "Sid" : "ConsoleLogSummaryObtainLogs",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  }
}
```

```
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCleanRoomsMLFullAccess

説明 : AWS Clean Rooms ML リソースへのフルアクセスと、関連する へのアクセスを許可します
AWS のサービス。

AWSCleanRoomsMLFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsMLFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 21:02 UTC
- 編集日時 : 2023 年 11 月 29 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCleanRoomsMLReadOnlyAccess

説明： AWS Clean Rooms ML リソースへの読み取り専用アクセスと、関連する AWS Clean Rooms リソースへの読み取り専用アクセスを許可する

AWSCleanRoomsMLReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCleanRoomsMLReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 29 日 20:55 UTC
- 編集日時: 2023 年 11 月 29 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCleanRoomsReadOnlyAccess

説明： AWS Clean Rooms リソースへの読み取り専用アクセスと、関連する AWS Glue および Amazon CloudWatch Logs リソースへの読み取り専用アクセスを許可します。

AWSCleanRoomsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCleanRoomsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 12 日 16:10 UTC

- 編集日時: 2023 年 1 月 12 日 16:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloud9Administrator

説明： AWS Cloud9 への管理者アクセスを提供します。

AWSCloud9Administrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9Administrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2017 年 11 月 30 日 16:17 UTC
- 編集日時: 2023 年 10 月 11 日 12:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9Administrator

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWS Cloud9EnvironmentMember

説明：AWS Cloud9 共有開発環境に招待する機能を提供します。

AWS Cloud9EnvironmentMember は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloud9EnvironmentMember` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 30 日 16:18 UTC
- 編集日時: 2023 年 10 月 11 日 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloud9ServiceRolePolicy

説明： AWS Cloud9 のサービスにリンクされたロールポリシー

AWSCloud9ServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 30 日 13:44 UTC
- 編集日時: 2022 年 1 月 17 日 14:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloud9SSMInstanceProfile

説明：このポリシーは、Cloud9 InstanceProfile が SSM セッションマネージャーを使用してインスタンスに接続できるようにするロールを にアタッチするために使用されます。

AWSCloud9SSMInstanceProfile は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9SSMInstanceProfile をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 14 日 11:40 UTC
- 編集日時: 2020 年 5 月 14 日 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloud9User

説明： AWS Cloud9 開発環境を作成し、所有環境を管理するアクセス許可を提供します。

AWSCloud9User は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloud9User をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2017 年 11 月 30 日 16:16 UTC
- 編集日時: 2023 年 10 月 11 日 13:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWS CloudFormationFullAccess

説明：へのフルアクセスを提供します AWS CloudFormation。

AWS CloudFormationFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudFormationFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 26 日 21:50 UTC
- 編集日時: 2019 年 7 月 26 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudFormationReadOnlyAccess

説明： AWS CloudFormation 経由で へのアクセスを提供します AWS Management Console。

AWSCloudFormationReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudFormationReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2019 年 11 月 13 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudFrontLogger

説明： Logs CloudFront への書き込みアクセス許可を Logger CloudWatch に付与します。

AWSCloudFrontLogger は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 6 月 12 日 20:15 UTC
- 編集日時: 2019 年 11 月 22 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudHSMFullAccess

説明：すべての CloudHSM リソースへのフルアクセスを提供します。

AWSCloudHSMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudHSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloudHSMReadOnlyAccess

説明 : すべての CloudHSM リソースへの読み取り専用アクセスを提供します。

AWSCloudHSMReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudHSMReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudHSMRole

説明： AWS CloudHSM サービスロールのデフォルトポリシー。

AWSCloudHSMRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudHSMRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudMapDiscoverInstanceAccess

説明： Map Discovery API AWS クラウド へのアクセスを提供します。

AWSCloudMapDiscoverInstanceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapDiscoverInstanceAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 00:02 UTC
- 編集日時: 2023 年 9 月 20 日 21:48 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudMapFullAccess

説明: すべての AWS クラウド マップアクションへのフルアクセスを提供します。

AWSCloudMapFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 23:57 UTC
- 編集日時: 2020 年 7 月 29 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudMapReadOnlyAccess

説明：すべての AWS クラウド マップアクションへの読み取り専用アクセスを提供します。

AWSCloudMapReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudMapReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 23:45 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudMapRegisterInstanceAccess

説明：AWS クラウド マップアクションへの登録者レベルのアクセスを提供します。

AWSCloudMapRegisterInstanceAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCloudMapRegisterInstanceAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 00:04 UTC
- 編集日時: 2023 年 9 月 20 日 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloudShellFullAccess

説明: すべての機能 AWS CloudShell で を使用する許可

AWSCloudShellFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudShellFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 18:07 UTC
- 編集日時: 2020 年 12 月 15 日 18:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCloudTrail_FullAccess

説明： へのフルアクセスを提供します AWS CloudTrail。

AWSCloudTrail_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudTrail_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 10 月 8 日 23:41 UTC
- 編集日時: 2021 年 2 月 22 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloudTrail_ReadOnlyAccess

説明： への読み取り専用アクセスを提供します AWS CloudTrail。

AWSCloudTrail_ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCloudTrail_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 6 月 14 日 17:19 UTC
- 編集日時: 2022 年 6 月 14 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

説明: このポリシーは、 という名前のサービスにリンクされたロールによって使用されます AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents。 は CloudWatch 、アラームが ALARM 状態になったときに、 CloudWatch このサービスにリンクされたロールを使用して AWS System Manager Incident Manager アクションを実行します。このポリシーは、ユーザーに代わって インシデントを開始するアクセス許可を付与します。

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 27 日 13:30 UTC
- 編集日時: 2021 年 4 月 27 日 13:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeArtifactAdminAccess

説明 : AWS CodeArtifact 経由でへのフルアクセスを提供します AWS Management Console。

AWSCodeArtifactAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeArtifactAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 6 月 16 日 23:53 UTC
- 編集日時: 2020 年 6 月 16 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeArtifactReadOnlyAccess

説明： AWS CodeArtifact 経由で への読み取り専用アクセスを提供します AWS Management Console。

AWSCodeArtifactReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeArtifactReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 25 日 21:23 UTC
- 編集日時: 2020 年 6 月 25 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeBuildAdminAccess

説明：AWS CodeBuild 経由でへのフルアクセスを提供します AWS Management Console。また、AmazonS3ReadOnlyAccess をアタッチしてビルドアーティファクトをダウンロードし、IAM をアタッチFullAccessしてのサービスロールを作成および管理します CodeBuild。

AWSCodeBuildAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:04 UTC
- 編集日時: 2024 年 5 月 2 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
```

```
    "events:ListTargetsByRule",
    "events:ListRuleNamesByTarget",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets",
    "logs:GetLogEvents",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "CWLDeleteLogGroupAccess",
  "Action" : [
    "logs:DeleteLogGroup"
  ],
  "Effect" : "Allow",
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:CreateConnection",
    "codestar-connections>DeleteConnection",
    "codestar-connections:UpdateConnectionInstallation",
    "codestar-connections:TagResource",
```

```
    "codestar-connections:UntagResource",
    "codestar-connections:ListConnections",
    "codestar-connections:ListInstallationTargets",
    "codestar-connections:ListTagsForResource",
    "codestar-connections:GetConnection",
    "codestar-connections:GetIndividualAccessToken",
    "codestar-connections:GetInstallationUrl",
    "codestar-connections:PassConnection",
    "codestar-connections:StartOAuthHandshake",
    "codestar-connections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications>DeleteNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsforResource"
  ],
  "Resource" : "*"
}
```

```
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeBuildDeveloperAccess

説明： AWS CodeBuild 経由でへのアクセスを許可しますが、AWS Management Console、CodeBuild プロジェクト管理は許可しません。またAmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

AWSCodeBuildDeveloperAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:02 UTC
- 編集日時: 2024 年 5 月 2 日 01:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
```

```
    "codebuild:BatchGet*",
    "codebuild:GetResourcePolicy",
    "codebuild:DescribeTestCases",
    "codebuild:DescribeCodeCoverages",
    "codebuild:List*",
    "codecommit:GetBranch",
    "codecommit:GetCommit",
    "codecommit:GetRepository",
    "codecommit:ListBranches",
    "cloudwatch:GetMetricStatistics",
    "events:DescribeRule",
    "events:ListTargetsByRule",
    "events:ListRuleNamesByTarget",
    "logs:GetLogEvents",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
},
{
  "Sid" : "SSMParameterWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
},
{
  "Sid" : "SSMStartSessionAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:StartSession"
  ],
  "Resource" : "arn:aws:ecs:*:*:task/*/*"
},
{
  "Sid" : "CodeStarConnectionsUserAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:ListConnections",
    "codestar-connections:GetConnection"
  ],
  "Resource" : [
```



```
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
},
{
  "Sid" : "CodeStarNotificationsReadWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:CreateNotificationRule",
    "codestar-notifications:DescribeNotificationRule",
    "codestar-notifications:UpdateNotificationRule",
    "codestar-notifications:Subscribe",
    "codestar-notifications:Unsubscribe"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
    }
  }
},
{
  "Sid" : "CodeStarNotificationsListAccess",
  "Effect" : "Allow",
  "Action" : [
    "codestar-notifications:ListNotificationRules",
    "codestar-notifications:ListEventTypes",
    "codestar-notifications:ListTargets",
    "codestar-notifications:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SNSTopicListAccess",
  "Effect" : "Allow",
  "Action" : [
    "sns:ListTopics",
    "sns:GetTopicAttributes"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarNotificationsChatbotAccess",
  "Effect" : "Allow",
```

```
    "Action" : [
      "chatbot:DescribeSlackChannelConfigurations",
      "chatbot:ListMicrosoftTeamsChannelConfigurations"
    ],
    "Resource" : "*"
  }
],
"Version" : "2012-10-17"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeBuildReadOnlyAccess

説明：AWS CodeBuild 経由でへの読み取り専用アクセスを提供します AWS Management Console。またAmazonS3ReadOnlyAccess をアタッチして、ビルドアーティファクトをダウンロードできるようにします。

AWSCodeBuildReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeBuildReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 19:03 UTC
- 編集日時: 2024 年 5 月 2 日 01:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v12 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    }
  ],
  {
    "Sid" : "CodeStarNotificationsListAccess",
    "Effect" : "Allow",
    "Action" : [
      "codestar-notifications:ListNotificationRules",
      "codestar-notifications:ListEventTypes",
      "codestar-notifications:ListTargets"
    ],
    "Resource" : "*"
  }
],
"Version" : "2012-10-17"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeCommitFullAccess

説明 : AWS CodeCommit 経由で へのフルアクセスを提供します AWS Management Console。

AWSCodeCommitFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeCommitFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2023 年 7 月 17 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeCommitPowerUser

説明： AWS CodeCommit リポジトリへのフルアクセスを提供しますが、リポジトリの削除は許可しません。

AWSCodeCommitPowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitPowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:06 UTC
- 編集日時: 2023 年 7 月 17 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

ポリシーのバージョン

ポリシーのバージョン: v15 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeCommitReadOnly

説明： AWS CodeCommit 経由で への読み取り専用アクセスを提供します AWS Management Console。

AWSCodeCommitReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeCommitReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:05 UTC
- 編集日時: 2021 年 8 月 18 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployDeployerAccess

説明： リビジョンを登録してデプロイするためのアクセスを提供します。

AWSCodeDeployDeployerAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployDeployerAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:18 UTC
- 編集日時: 2020 年 4 月 2 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployFullAccess

説明： CodeDeploy リソースへのフルアクセスを提供します。

AWSCodeDeployFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:13 UTC
- 編集日時: 2020 年 4 月 2 日 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployReadOnlyAccess

説明： CodeDeploy リソースへの読み取り専用アクセスを提供します。

AWSCodeDeployReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 5 月 19 日 18:21 UTC
- 編集日時: 2020 年 4 月 2 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRole

説明： タグを拡張し、ユーザーに代わって Auto Scaling とやり取りするための CodeDeploy サービスアクセスを提供します。

AWSCodeDeployRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 5 月 4 日 18:05 UTC
- 編集日時: 2023 年 8 月 16 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRoleForCloudFormation

説明： を通じてブルー/グリーンデプロイを実行するために、ユーザーに代わって Lambda 関数を呼び出すための CodeDeploy サービスアクセスを提供します CloudFormation。

AWSCodeDeployRoleForCloudFormation は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForCloudFormation をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 17:12 UTC
- 編集日時: 2020 年 5 月 19 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "lambda:InvokeFunction"
    ],
    "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
    "Effect" : "Allow"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRoleForECS

説明：ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための CodeDeploy サービス全体のアクセスを提供します。すべての S3 オブジェクトの読み取り、すべての Lambda 関数の呼び出し、アカウント内のすべての SNS トピックへの公開、すべての ECS サービスの更新など、サポートサービスへのフルアクセスを許可します。

AWSCodeDeployRoleForECS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForECS をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 20:40 UTC
- 編集日時: 2019 年 9 月 23 日 22:37 UTC

- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRoleForECSLimited

説明：ユーザーに代わって ECS ブルー/グリーンデプロイを実行するための CodeDeploy サービス制限付きアクセスを提供します。

AWSCodeDeployRoleForECSLimited は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForECSLimited をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 20:42 UTC
- 編集日時: 2019 年 9 月 23 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRoleForLambda

説明：ユーザーに代わって Lambda デプロイを実行するための CodeDeploy サービスアクセスを提供します。

AWSCodeDeployRoleForLambda は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambda をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 28 日 14:05 UTC
- 編集日時: 2019 年 12 月 3 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeDeployRoleForLambdaLimited

説明: ユーザーに代わって Lambda デプロイを実行するための CodeDeploy サービス制限付きアクセスを提供します。

AWSCodeDeployRoleForLambdaLimited は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeDeployRoleForLambdaLimited をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 17 日 17:14 UTC
- 編集日時: 2020 年 8 月 17 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodePipeline_FullAccess

説明： AWS CodePipeline 経由で へのフルアクセスを提供します AWS Management Console。

AWSCodePipeline_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipeline_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 3 日 22:38 UTC
- 編集日時: 2024 年 3 月 14 日 17:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodePipeline_ReadOnlyAccess

説明： AWS CodePipeline 経由で への読み取り専用アクセスを提供します AWS Management Console。

AWSCodePipeline_ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipeline_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 3 日 22:25 UTC
- 編集日時: 2020 年 8 月 3 日 22:25 UTC

- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodePipelineApproverAccess

説明：すべてのパイプラインの手動変更を表示および承認するためのアクセスを提供します

AWSCodePipelineApproverAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineApproverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 7 月 28 日 18:59 UTC
- 編集日時: 2017 年 8 月 2 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodePipelineCustomActionAccess

説明: ジョブの詳細 (一時的な認証情報を含む) をポーリングし、ステータスの更新を にレポートするカスタムアクションへのアクセスを提供します AWS CodePipeline。

AWSCodePipelineCustomActionAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodePipelineCustomActionAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:02 UTC
- 編集日時: 2015 年 7 月 9 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeStarFullAccess

説明： AWS CodeStar 経由でへのフルアクセスを提供します AWS Management Console。

AWSCodeStarFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCodeStarFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 4 月 19 日 16:23 UTC
- 編集日時: 2023 年 3 月 28 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCodeStarNotificationsServiceRolePolicy

説明：AWS CodeStar 通知がユーザーに代わって Amazon CloudWatch Events にアクセスすることを許可する

AWSCodeStarNotificationsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 5 日 16:10 UTC
- 編集日時: 2020 年 3 月 19 日 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCodeStarServiceRole

説明：使用禁止 - お客様に代わって が IAM およびその他の AWS CodeStar サービスリソースを管理する CodeStar ための管理権限を付与するサービスロールポリシー。

AWSCodeStarServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCodeStarServiceRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 4 月 19 日 15:20 UTC
- 編集日時: 2021 年 9 月 20 日 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCompromisedKeyQuarantine

説明: IAM ユーザーの認証情報が侵害されたり、公開されたりした場合に AWS、チームによって適用される特定のアクションへのアクセスを拒否します。このポリシーは削除しないでください。代わりに、このイベントに関して送信されたメールで指示されている手順に従ってください。

AWSCompromisedKeyQuarantine は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCompromisedKeyQuarantine をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 11 日 18:04 UTC
- 編集日時: 2020 年 8 月 11 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSCompromisedKeyQuarantineV2

説明: IAM ユーザーの認証情報が侵害されたり、公開されたりした場合に AWS、チームによって適用される特定のアクションへのアクセスを拒否します。このポリシーは削除しないでください。代わりに、このイベントに関して作成したサポートケースに明記されている指示に従ってください。

AWSCompromisedKeyQuarantineV2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSCompromisedKeyQuarantineV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 4 月 21 日 22:30 UTC
- 編集日時: 2023 年 3 月 16 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSConfigMultiAccountSetupPolicy

説明： Config が AWS サービスを呼び出し、組織全体に Config リソースをデプロイすることを許可する

AWSConfigMultiAccountSetupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 17 日 18:03 UTC
- 編集日時: 2023 年 2 月 24 日 01:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSConfigRemediationServiceRolePolicy

説明：AWS Config がユーザーに代わって非準拠のリソースを修復できるようにします。

AWSConfigRemediationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 18 日 21:21 UTC
- 編集日時: 2019 年 6 月 18 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSConfigRoleForOrganizations

説明： AWS Config が読み取り専用の AWS Organizations APIs を呼び出すことを許可します

AWSConfigRoleForOrganizations は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigRoleForOrganizations をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 3 月 19 日 22:53 UTC
- 編集日時: 2020 年 11 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSConfigRulesExecutionRole

説明 : AWS Lambda 関数が AWS Config API および Config が Amazon S3 に定期的に AWS 配信する設定スナップショットにアクセスできるようにします。このアクセスは、カスタム Config ルールの設定変更を評価する関数に必要です。

AWSConfigRulesExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigRulesExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 3 月 25 日 17:59 UTC
- 編集日時: 2019 年 5 月 13 日 21:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSConfigServiceRolePolicy

説明： Config がユーザーに代わって AWS サービスを呼び出し、リソース設定を収集できるようにします。

AWSConfigServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 5 月 30 日 23:31 UTC
- 編集日時: 2024 年 2 月 22 日 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v50 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSConfigUserAccess

説明： リソースのタグによる検索やすべてのタグの読み取りなど、AWS Config を使用するためのアクセスを提供します。これは、管理者権限を必要とする AWS Config を設定するアクセス許可を提供しません。

AWSConfigUserAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConfigUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 18 日 19:38 UTC
- 編集日時: 2019 年 3 月 18 日 20:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSConnector

説明: AWS Connector がユーザーに代わって VMs をインポートできるように、すべての EC2 オブジェクトへの広範な読み取り/書き込みアクセス、'import-to-ec2-' で S3 始まる S3 バケットへの読み取り/書き込みアクセス、およびすべての S3 バケットを一覧表示する機能を有効にします。

AWSConnector は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSConnector をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 11 日 17:14 UTC
- 編集日時: 2015 年 9 月 28 日 19:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSControlTowerAccountServiceRolePolicy

説明：AWS Control Tower がユーザーに代わって自動アカウント設定と一元化されたガバナンスを提供する AWS サービスを呼び出すことを許可します。

AWSControlTowerAccountServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 5 日 22:04 UTC
- 編集日時: 2023 年 6 月 5 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSControlTowerServiceRolePolicy

説明 : AWS Control Tower が管理または使用する AWS リソースへのアクセスを提供します

AWSControlTowerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSControlTowerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 5 月 3 日 18:19 UTC
- 編集日時: 2023 年 4 月 12 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSCostAndUsageReportAutomationPolicy

説明：アカウントの組織を記述し、MAP プログラムの S3 バケットを作成してタグを適用し、コストと使用状況レポートを作成し、コストと使用状況レポートの定義を記述するアクセス許可を に付与します。

AWSCostAndUsageReportAutomationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSCostAndUsageReportAutomationPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 1 日 21:27 UTC
- 編集日時: 2021 年 11 月 1 日 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDataExchangeFullAccess

説明: AWS Management Console および SDK を使用して AWS Data Exchange および AWS Marketplace アクションへのフルアクセスを許可します。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

AWSDataExchangeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 5 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
  },
  {
    "Sid" : "S3GetActionConditionalTagAndADX",
    "Effect" : "Allow",
    "Action" : "s3:GetObject",
    "Resource" : "*",
    "Condition" : {
      "StringEqualsIgnoreCase" : {
        "s3:ExistingObjectTag/AWSDataExchange" : "true"
      },
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "S3WriteActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource" : "arn:aws:s3::*aws-data-exchange*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "dataexchange.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "S3ReadActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
```

```
"Sid" : "AWSMarketplaceProviderActions",
"Effect" : "Allow",
"Action" : [
  "aws-marketplace:DescribeEntity",
  "aws-marketplace:ListEntities",
  "aws-marketplace:StartChangeSet",
  "aws-marketplace:ListChangeSets",
  "aws-marketplace:DescribeChangeSet",
  "aws-marketplace:CancelChangeSet",
  "aws-marketplace:GetAgreementApprovalRequest",
  "aws-marketplace:ListAgreementApprovalRequests",
  "aws-marketplace:AcceptAgreementApprovalRequest",
  "aws-marketplace:RejectAgreementApprovalRequest",
  "aws-marketplace:UpdateAgreementApprovalRequest",
  "aws-marketplace:SearchAgreements",
  "aws-marketplace:GetAgreementTerms",
  "aws-marketplace:TagResource",
  "aws-marketplace:UntagResource",
  "aws-marketplace:ListTagsForResource"
],
"Resource" : "*"
},
{
  "Sid" : "AWSMarketplaceSubscriberActions",
  "Effect" : "Allow",
  "Action" : [
    "aws-marketplace:Subscribe",
    "aws-marketplace:Unsubscribe",
    "aws-marketplace:ViewSubscriptions",
    "aws-marketplace:GetAgreementRequest",
    "aws-marketplace:ListAgreementRequests",
    "aws-marketplace:CancelAgreementRequest",
    "aws-marketplace:ListPrivateListings",
    "aws-marketplace:GetPrivateListing",
    "aws-marketplace:DescribeAgreement"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KMSActions",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:ListAliases",
```

```
    "kms:ListKeys"
  ],
  "Resource" : "*"
},
{
  "Sid" : "RedshiftConditionalActions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:AuthorizeDataShare"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "redshift:ConsumerIdentifier" : "ADX"
    }
  }
},
{
  "Sid" : "RedshiftActions",
  "Effect" : "Allow",
  "Action" : [
    "redshift:DescribeDataSharesForProducer",
    "redshift:DescribeDataShares"
  ],
  "Resource" : "*"
},
{
  "Sid" : "APIGatewayActions",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDataExchangeProviderFullAccess

説明: AWS Management Console および SDK を使用して、データプロバイダーに AWS Data Exchange および AWS Marketplace アクションへのアクセスを許可します。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

AWSDataExchangeProviderFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeProviderFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2022 年 3 月 15 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDataExchangeReadOnly

説明: AWS Management Console および SDK を使用して AWS Data Exchange および AWS Marketplace アクションへの読み取り専用アクセスを許可します。

AWSDataExchangeReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2021 年 5 月 10 日 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDataExchangeSubscriberFullAccess

説明： AWS Management Console および SDK を使用して、データサブスクライバーに AWS Data Exchange および AWS Marketplace アクションへのアクセスを許可します。また、AWS Data Exchange を最大限に活用するために必要な関連サービスへの選択アクセスも提供します。

AWSDataExchangeSubscriberFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataExchangeSubscriberFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 13 日 19:27 UTC
- 編集日時: 2024 年 5 月 21 日 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange>DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    }
  ],
  {
    "Sid" : "S3ReadActions",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "AWSMarketplaceSubscriberActions",
    "Effect" : "Allow",
    "Action" : [
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe",
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:GetAgreementRequest",
      "aws-marketplace:ListAgreementRequests",
      "aws-marketplace:CancelAgreementRequest",
      "aws-marketplace:ListPrivateListings"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KMSActions",
    "Effect" : "Allow",
    "Action" : [
      "kms:DescribeKey",
      "kms:ListAliases",
```

```
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDataLifecycleManagerServiceRole

説明： AWS リソースに対してアクションを実行するための適切なアクセス許可を AWS Data Lifecycle Manager に提供します

AWSDataLifecycleManagerServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataLifecycleManagerServiceRole をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 6 日 19:34 UTC
- 編集日時: 2022 年 9 月 19 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

説明: AMI 管理の AWS リソースに対してアクションを実行するための適切なアクセス許可を AWS Data Lifecycle Manager に提供します

AWSDataLifecycleManagerServiceRoleForAMIManagement は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSDataLifecycleManagerServiceRoleForAMIManagement をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 10 月 21 日 19:39 UTC
- 編集日時: 2021 年 8 月 19 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDataLifecycleManagerSSMFullAccess

説明：すべての Amazon EC2 インスタンスで事前スクリプトと事後スクリプトを実行するために必要な Systems Manager アクションを実行するアクセス許可を Amazon Data Lifecycle Manager に付与します。

AWSDataLifecycleManagerSSMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataLifecycleManagerSSMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 10 月 31 日 20:29 UTC
- 編集日時: 2023 年 11 月 16 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDatapipeline_FullAccess

説明: Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールの一覧表示、デフォルトのロールの passRole アクセスを提供します。

AWSDatapipeline_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDatapipeline_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 19 日 23:14 UTC
- 編集日時: 2017 年 8 月 17 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDatapipeline_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDatapipeline_PowerUser

説明: Data Pipeline へのフルアクセス、S3、DynamoDB、Redshift、RDS、SNS、IAM ロールの一覧表示、デフォルトのロールの passRole アクセスを提供します。

AWSDatapipeline_PowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDatapipeline_PowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 19 日 23:16 UTC
- 編集日時: 2017 年 8 月 17 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDataSyncDiscoveryServiceRolePolicy

説明： DataSync Discovery がユーザーに代わって他の AWS サービスと統合できるようにします。

AWSDataSyncDiscoveryServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 20 日 22:19 UTC
- 編集日時: 2023 年 3 月 20 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDataSyncFullAccess

説明： へのフルアクセス AWS DataSync と依存関係への最小限のアクセスを提供します

AWSDataSyncFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataSyncFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 19:40 UTC
- 編集日時: 2024 年 2 月 16 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDataSyncReadOnlyAccess

説明： への読み取り専用アクセスを提供します AWS DataSync

AWSDataSyncReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDataSyncReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 18 日 19:18 UTC
- 編集日時: 2020 年 6 月 30 日 17:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-FleetWorker

説明： Deadline Cloud AWS ワーカーにファームでタスクを実行するためのアクセスを提供します。

AWSDeadlineCloud-FleetWorker は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-FleetWorker をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:21 UTC
- 編集日時: 2024 年 4 月 1 日 17:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ]
    }
  ]
}
```



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-UserAccessFarms

説明 : Deadline Cloud AWS ファームへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための読み取り専用アクセス許可を制限します。このポリシーをスタジオに関連付けられたユーザーロールにアタッチします。

AWSDeadlineCloud-UserAccessFarms は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessFarms をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 16:54 UTC
- 編集日時: 2024 年 4 月 1 日 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline>CreateBudget",
        "deadline>DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",

```

```
    "deadline:GetSessionsStatisticsAggregation",
    "deadline:ListBudgets",
    "deadline:StartSessionsStatisticsAggregation",
    "deadline:UpdateBudget"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FarmMembershipLevels" : [
        "OWNER"
      ]
    }
  }
},
{
  "Sid" : "ManagerLevelMemberAssociation",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssociateMemberToFarm",
    "deadline:AssociateMemberToFleet",
    "deadline:AssociateMemberToJob",
    "deadline:AssociateMemberToQueue"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FarmMembershipLevels" : [
        "MANAGER"
      ]
    }
  },
  "StringEquals" : {
    "deadline:AssociatedMembershipLevel" : [
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER",
      ""
    ]
  },
  "deadline:MembershipLevel" : [
    "MANAGER",
    "CONTRIBUTOR",
```

```
        "VIEWER"
      ]
    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:DisassociateMemberFromFarm",
      "deadline:DisassociateMemberFromFleet",
      "deadline:DisassociateMemberFromJob",
      "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ]
      }
    }
  },
  {
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "deadline:ListFarmMembers",
      "deadline:ListFleetMembers",
      "deadline:ListJobMembers",
      "deadline:ListQueueMembers",
      "deadline:UpdateJob",
      "deadline:UpdateSession",
      "deadline:UpdateStep",
```

```
    "deadline:UpdateTask"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FarmMembershipLevels" : [
        "OWNER",
        "MANAGER"
      ]
    }
  }
},
{
  "Sid" : "OwnerManagerContributorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssumeQueueRoleForUser",
    "deadline:CreateJob"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FarmMembershipLevels" : [
        "OWNER",
        "MANAGER",
        "CONTRIBUTOR"
      ]
    }
  }
},
{
  "Sid" : "AllLevelsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssumeFleetRoleForRead",
    "deadline:AssumeQueueRoleForRead",
    "deadline:GetFarm",
    "deadline:GetFleet",
    "deadline:GetJob",
    "deadline:GetQueue",
```

```
    "deadline:GetQueueEnvironment",
    "deadline:GetQueueFleetAssociation",
    "deadline:GetSession",
    "deadline:GetSessionAction",
    "deadline:GetStep",
    "deadline:GetStorageProfile",
    "deadline:GetStorageProfileForQueue",
    "deadline:GetTask",
    "deadline:GetWorker",
    "deadline:ListQueueEnvironments",
    "deadline:ListQueueFleetAssociations",
    "deadline:ListSessionActions",
    "deadline:ListSessions",
    "deadline:ListSessionsForWorker",
    "deadline:ListStepConsumers",
    "deadline:ListStepDependencies",
    "deadline:ListSteps",
    "deadline:ListStorageProfiles",
    "deadline:ListStorageProfilesForQueue",
    "deadline:ListTasks",
    "deadline:ListWorkers",
    "deadline:SearchJobs",
    "deadline:SearchSteps",
    "deadline:SearchTasks",
    "deadline:SearchWorkers"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FarmMembershipLevels" : [
        "OWNER",
        "MANAGER",
        "CONTRIBUTOR",
        "VIEWER"
      ]
    }
  }
},
{
  "Sid" : "ListBasedOnMembership",
  "Effect" : "Allow",
  "Action" : [
```

```
    "deadline:ListFarms",
    "deadline:ListFleets",
    "deadline:ListJobs",
    "deadline:ListQueues"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
    }
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-UserAccessFleets

説明: Deadline Cloud AWS フリートへのユーザーワークステーションアクセスに、他の必要なサービスを呼び出すための読み取り専用アクセス許可が制限されています。このポリシーをスタジオに関連付けられたユーザーロールにアタッチします。

AWSDeadlineCloud-UserAccessFleets は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessFleets をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2024 年 4 月 1 日 17:01 UTC
- 編集日時: 2024 年 4 月 1 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```



```
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FleetMembershipLevels" : [
          "OWNER"
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:AssociateMemberToFleet"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FleetMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ],
        "deadline:MembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER"
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:DisassociateMemberFromFleet"
```

```
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FleetMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ]
        }
    }
},
{
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListFleetMembers"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:FleetMembershipLevels" : [
                "OWNER",
                "MANAGER"
            ]
        }
    }
},
{
    "Sid" : "AllLevelsPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
```

```
    "deadline:GetQueueFleetAssociation",
    "deadline:GetWorker",
    "deadline:ListQueueFleetAssociations",
    "deadline:ListSessionsForWorker",
    "deadline:ListWorkers",
    "deadline:SearchWorkers"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:FleetMembershipLevels" : [
        "OWNER",
        "MANAGER",
        "CONTRIBUTOR",
        "VIEWER"
      ]
    }
  }
},
{
  "Sid" : "ListBasedOnMembership",
  "Effect" : "Allow",
  "Action" : [
    "deadline:ListFleets"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-UserAccessJobs

説明: Deadline Cloud AWS ジョブへのユーザーワークステーションアクセスに、他の必要なサービス呼び出すための読み取り専用アクセス許可が制限されています。このポリシーをスタジオに関連付けられたユーザーロールにアタッチします。

AWSDeadlineCloud-UserAccessJobs は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-UserAccessJobs をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:05 UTC
- 編集日時: 2024 年 4 月 1 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Effect" : "Allow",
"Action" : [
  "identitystore:DescribeGroup",
  "identitystore:DescribeUser",
  "identitystore:ListGroupMembershipsForMember",
  "deadline:GetApplicationVersion",
  "ec2:DescribeInstanceTypes",
  "identitystore:ListUsers"
],
"Resource" : [
  "*"
]
},
{
  "Sid" : "OwnerLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssociateMemberToJob",
    "deadline:DisassociateMemberFromJob"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:JobMembershipLevels" : [
        "OWNER"
      ]
    }
  }
},
{
  "Sid" : "ManagerLevelMemberAssociation",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssociateMemberToJob"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:JobMembershipLevels" : [
        "MANAGER"
      ]
    }
  }
}
```

```
    ]
  },
  "StringEquals" : {
    "deadline:AssociatedMembershipLevel" : [
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER",
      ""
    ],
    "deadline:MembershipLevel" : [
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER"
    ]
  }
},
{
  "Sid" : "ManagerLevelMemberDisassociation",
  "Effect" : "Allow",
  "Action" : [
    "deadline:DisassociateMemberFromJob"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:JobMembershipLevels" : [
        "MANAGER"
      ]
    }
  },
  "StringEquals" : {
    "deadline:AssociatedMembershipLevel" : [
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER",
      ""
    ]
  }
},
{
  "Sid" : "OwnerManagerPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "deadline:ListJobMembers",
  "deadline:UpdateJob",
  "deadline:UpdateSession",
  "deadline:UpdateStep",
  "deadline:UpdateTask"
],
"Resource" : [
  "*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "deadline:JobMembershipLevels" : [
      "OWNER",
      "MANAGER"
    ]
  }
}
},
{
  "Sid" : "AllLevelsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:GetJob",
    "deadline:GetSession",
    "deadline:GetSessionAction",
    "deadline:GetStep",
    "deadline:GetTask",
    "deadline:ListSessionActions",
    "deadline:ListSessions",
    "deadline:ListStepConsumers",
    "deadline:ListStepDependencies",
    "deadline:ListSteps",
    "deadline:ListTasks",
    "deadline:SearchSteps",
    "deadline:SearchTasks"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:JobMembershipLevels" : [
```

```
        "OWNER",
        "MANAGER",
        "CONTRIBUTOR",
        "VIEWER"
    ]
}
},
{
    "Sid" : "ListBasedOnMembership",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListJobs"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
    }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-UserAccessQueues

説明 : Deadline Cloud AWS キューへのユーザーワークステーションアクセスに、他の必要なサービス呼び出すための読み取り専用アクセス許可を制限します。このポリシーをスタジオに関連付けられたユーザーロールにアタッチします。

AWSDeadlineCloud-UserAccessQueues は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeadlineCloud-UserAccessQueues` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:10 UTC
- 編集日時: 2024 年 4 月 1 日 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```
{
  "Sid" : "OwnerLevelPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssociateMemberToJob",
    "deadline:AssociateMemberToQueue",
    "deadline:DisassociateMemberFromJob",
    "deadline:DisassociateMemberFromQueue"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:QueueMembershipLevels" : [
        "OWNER"
      ]
    }
  }
},
{
  "Sid" : "ManagerLevelMemberAssociation",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssociateMemberToJob",
    "deadline:AssociateMemberToQueue"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:QueueMembershipLevels" : [
        "MANAGER"
      ]
    }
  },
  "StringEquals" : {
    "deadline:AssociatedMembershipLevel" : [
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER",
      ""
    ]
  },
  "deadline:MembershipLevel" : [
```

```
        "MANAGER",
        "CONTRIBUTOR",
        "VIEWER"
    ]
}
},
{
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "deadline:QueueMembershipLevels" : [
                "MANAGER"
            ]
        },
        "StringEquals" : {
            "deadline:AssociatedMembershipLevel" : [
                "MANAGER",
                "CONTRIBUTOR",
                "VIEWER",
                ""
            ]
        }
    }
},
{
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
    ],
```

```
"Resource" : [
  "*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "deadline:QueueMembershipLevels" : [
      "OWNER",
      "MANAGER"
    ]
  }
},
{
  "Sid" : "OwnerManagerContributorPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssumeQueueRoleForUser",
    "deadline:CreateJob"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "deadline:QueueMembershipLevels" : [
        "OWNER",
        "MANAGER",
        "CONTRIBUTOR"
      ]
    }
  }
},
{
  "Sid" : "AllLevelsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "deadline:AssumeQueueRoleForRead",
    "deadline:GetJob",
    "deadline:GetQueue",
    "deadline:GetQueueEnvironment",
    "deadline:GetQueueFleetAssociation",
    "deadline:GetSession",
    "deadline:GetSessionAction",
    "deadline:GetStep",
```

```
"deadline:GetStorageProfileForQueue",
"deadline:GetTask",
"deadline:ListQueueEnvironments",
"deadline:ListQueueFleetAssociations",
"deadline:ListSessionActions",
"deadline:ListSessions",
"deadline:ListStepConsumers",
"deadline:ListStepDependencies",
"deadline:ListSteps",
"deadline:ListStorageProfilesForQueue",
"deadline:ListTasks",
"deadline:SearchJobs",
"deadline:SearchSteps",
"deadline:SearchTasks"
],
"Resource" : [
  "*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "deadline:QueueMembershipLevels" : [
      "OWNER",
      "MANAGER",
      "CONTRIBUTOR",
      "VIEWER"
    ]
  }
}
},
{
  "Sid" : "ListBasedOnMembership",
  "Effect" : "Allow",
  "Action" : [
    "deadline:ListJobs",
    "deadline:ListQueues"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringEquals" : {
      "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
    }
  }
}
```

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeadlineCloud-WorkerHost

説明: AWS Deadline Cloud ワーカーホストがファーム内のフリートに参加するためのアクセスを提供します。

AWSDeadlineCloud-WorkerHost は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeadlineCloud-WorkerHost をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 4 月 1 日 17:28 UTC
- 編集日時: 2024 年 4 月 1 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepLensLambdaFunctionAccessPolicy

説明：このポリシーは、DeepLens デバイスで実行される DeepLens 管理 Lambda 関数に必要なアクセス許可を指定します。

AWSDeepLensLambdaFunctionAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSDeepLensLambdaFunctionAccessPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 15:47 UTC
- 編集日時: 2019 年 6 月 11 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepLensServiceRolePolicy

説明 : IoT AWS のサービス、S3、AWS Lambda など、DeepLens に必要な、リソース、ロール、GreenGrass およびその依存関係 AWS DeepLens へのアクセスを許可します。IoT

AWSDeepLensServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepLensServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 15:46 UTC
- 編集日時: 2019 年 9 月 25 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerAccountAdminAccess

説明: マルチユーザーモードとシングルユーザーモードの切り替えを含む、すべてのアクションへの DeepRacer 管理者アクセス。

AWSDeepRacerAccountAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerAccountAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Condition" : {
      "Null" : {
        "deepracer:UserToken" : "true"
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerCloudFormationAccessPolicy

説明： CloudFormation がユーザーに代わって AWS スタックとリソースを作成および管理できるようにします。

AWSDeepRacerCloudFormationAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerCloudFormationAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 6 月 14 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerDefaultMultiUserAccess

説明： マルチユーザーモードで DeepRacer を使用するための DeepRacer MultiUser デフォルトのユーザーアクセス

AWSDeepRacerDefaultMultiUserAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerDefaultMultiUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 28 日 01:27 UTC
- 編集日時: 2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "deepracer:Add*",
      "deepracer:Remove*",
      "deepracer:Create*",
      "deepracer:Perform*",
      "deepracer:Clone*",
      "deepracer:Get*",
      "deepracer:List*",
      "deepracer>Edit*",
      "deepracer:Start*",
      "deepracer:Set*",
      "deepracer:Update*",
      "deepracer>Delete*",
      "deepracer:Stop*",
      "deepracer:Import*",
      "deepracer:Tag*",
      "deepracer:Untag*"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "Null" : {
        "deepracer:UserToken" : "false"
      },
      "Bool" : {
        "deepracer:MultiUser" : "true"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "deepracer:GetAccountConfig",
      "deepracer:GetTrack",
      "deepracer:ListTracks",
      "deepracer:TestRewardFunction"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```



```
    ]
  },
  {
    "Effect" : "Deny",
    "Action" : [
      "deepracer:Admin*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerFullAccess

説明： へのフルアクセスを提供します AWS DeepRacer。また、関連サービス (S3 など) への限定アクセスも提供します。

AWSDeepRacerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 5 日 22:03 UTC
- 編集日時: 2020 年 10 月 5 日 22:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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::*deeperacer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3::*DeepRacer/*",
        "arn:aws:s3::*Deepracer/*",
        "arn:aws:s3::*deeperacer/*",
        "arn:aws:s3:::dr-/*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerRoboMakerAccessPolicy

説明： RoboMaker がユーザーに代わって必要なリソースを作成し、AWS サービスを呼び出すことを許可します。

AWSDeepRacerRoboMakerAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerRoboMakerAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 2 月 28 日 21:59 UTC
- 編集日時: 2019 年 2 月 28 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeepRacerServiceRolePolicy

説明： DeepRacer がユーザーに代わって必要なリソースを作成し、AWS サービスを呼び出すことを許可します。

AWSDeepRacerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeepRacerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 2 月 28 日 21:58 UTC
- 編集日時: 2019 年 6 月 12 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

ポリシーのバージョニング

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDenyAll

説明: すべてのアクセスを拒否します。

AWSDenyAll は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDenyAll をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 1 日 22:36 UTC
- 編集日時: 2023 年 12 月 18 日 16:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Sid" : "DenyAll",
  "Effect" : "Deny",
  "Action" : [
    "*"
  ],
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeviceFarmFullAccess

説明：すべての AWS Device Farm オペレーションへのフルアクセスを提供します。

AWSDeviceFarmFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDeviceFarmFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 13 日 16:37 UTC
- 編集日時: 2015 年 7 月 13 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDeviceFarmServiceRolePolicy

説明：ユーザーに代わって EC2 Network API を呼び出すアクセス許可を AWS Device Farm に付与します。 APIs

AWSDeviceFarmServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 20 日 21:02 UTC
- 編集日時: 2022 年 9 月 20 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDeviceFarmTestGridServiceRolePolicy

説明：ユーザーに代わって EC2 API を呼び出すアクセス許可を AWS Device Farm に付与します。

APIs

AWSDeviceFarmTestGridServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 26 日 22:01 UTC
- 編集日時: 2021 年 5 月 26 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDirectConnectFullAccess

説明： 経由で AWS Direct Connect へのフルアクセスを提供します AWS Management Console。

AWSDirectConnectFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectConnectFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC

- 編集日時: 2019 年 4 月 30 日 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDirectConnectReadOnlyAccess

説明： 経由で AWS Direct Connect への読み取り専用アクセスを提供します AWS Management Console。

AWSDirectConnectReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectConnectReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2020 年 5 月 18 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ]
    }
  ],
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDirectConnectServiceRolePolicy

説明：ユーザーに代わってリソースを作成および管理するための AWS Direct Connect アクセス許可 AWS を提供します。

AWSDirectConnectServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 1 月 14 日 18:35 UTC
- 編集日時: 2021 年 1 月 14 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDirectoryServiceFullAccess

説明 : AWS Directory Service へのフルアクセスを提供します。

AWSDirectoryServiceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectoryServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 4 月 2 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
```

```
    "sns:ListTopics",
    "iam:ListRoles",
    "organizations:ListAccountsForParent",
    "organizations:ListRoots",
    "organizations:ListAccounts",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DirectoryServiceEventTopic",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns>DeleteTopic",
    "sns:SetTopicAttributes",
    "sns:Subscribe",
    "sns:Unsubscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
},
{
  "Sid" : "DirectoryServiceOrganizations",
  "Effect" : "Allow",
  "Action" : [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "ds.amazonaws.com"
    }
  }
},
{
  "Sid" : "DirectoryServiceTags",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ]
}
```



```
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDirectoryServiceReadOnlyAccess

説明： AWS Directory Service への読み取り専用アクセスを提供します。

AWSDirectoryServiceReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDirectoryServiceReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2018 年 9 月 25 日 21:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDiscoveryContinuousExportFirehosePolicy

説明： AWS Discovery Continuous Export に必要な AWS リソースへの書き込みアクセスを提供します

AWSDiscoveryContinuousExportFirehosePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSDiscoveryContinuousExportFirehosePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 8 月 9 日 18:29 UTC
- 編集日時: 2021 年 6 月 8 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSDMSFleetAdvisorServiceRolePolicy

説明： DMS Fleet Advisor がユーザーに代わって CloudWatch メトリクスを管理できるようにします。

AWS*DMS*FleetAdvisorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 6 日 09:10 UTC
- 編集日時: 2023 年 3 月 6 日 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSDMSServerlessServiceRolePolicy

説明：ユーザーに代わってアカウントで AWS DMS リソースを作成および管理するための DMS Serverless アクセス許可を付与します

AWSDMSServerlessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 18 日 20:28 UTC
- 編集日時: 2023 年 5 月 18 日 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSEC2CapacityReservationFleetRolePolicy

説明 : EC2 CapacityReservation Fleet サービスがキャパシティ予約を管理できるようにします

AWSEC2CapacityReservationFleetRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 29 日 14:43 UTC
- 編集日時: 2021 年 9 月 29 日 14:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSEC2FleetServiceRolePolicy

説明： EC2 フリート がインスタンスを起動および管理できるようにします。

AWSEC2FleetServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 21 日 00:08 UTC
- 編集日時: 2020 年 5 月 4 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSEC2SpotFleetServiceRolePolicy

説明： EC2 スポットフリートがスポットフリートインスタンスを起動および管理することを許可する

AWSEC2SpotFleetServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 23 日 19:13 UTC
- 編集日時: 2020 年 3 月 16 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSEC2SpotServiceRolePolicy

説明： EC2 スポットがスポットインスタンスを起動および管理することを許可する

AWSEC2SpotServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 18 日 18:51 UTC
- 編集日時: 2018 年 12 月 12 日 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSEC2VssSnapshotPolicy

説明: このポリシーは、Amazon EC2 Windows インスタンスにアタッチされている IAM ロールにアタッチされ、Amazon EC2 VSS ソリューションが Amazon マシンイメージ (AMI) と EBS スナップショットにタグを作成して追加できるようにします。

AWSEC2VssSnapshotPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEC2VssSnapshotPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 16:32 UTC
- 編集日時: 2024 年 3 月 27 日 16:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    }
  ],
}
```

```
{
  "Sid" : "CreateSnapshotsAccessInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
    }
  }
},
{
  "Sid" : "CreateSnapshotsAccessVolume",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshots"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "CreateImageWithTag",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateImage"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:RequestTag/AwsVssConfig" : "*"
    }
  }
},
{
  "Sid" : "CreateImageAccessInstance",
  "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateImage"
],
"Resource" : [
  "arn:aws:ec2:*:*:instance/*"
],
"Condition" : {
  "StringLike" : {
    "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
  }
}
},
{
  "Sid" : "CreateTagsOnResourceCreation",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateImage",
        "CreateSnapshots"
      ]
    }
  }
},
{
  "Sid" : "CreateTagsAfterResourceCreation",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/AwsVssConfig" : "*"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "AppConsistent",
```

```
        "Device"
      ]
    }
  },
  {
    "Sid" : "DescribeImagesAndSnapshots",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSECRPullThroughCache_ServiceRolePolicy

説明： AWS ECR プルスルーキャッシュによって使用または管理される AWS サービスとリソースへのアクセスを有効にする

AWSECRPullThroughCache_ServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2021 年 11 月 26 日 21:51 UTC
- 編集日時: 2023 年 11 月 13 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

説明: EC2 インスタンスの起動、EBS スナップショットと AMI の作成、Amazon CloudWatch Logs へのログのストリーミング、Amazon S3 へのアーティファクトの保存を行うアクセス許可をカスタムプラットフォームビルダー環境のインスタンスに付与します。

AWSElasticBeanstalkCustomPlatformforEC2Role は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkCustomPlatformforEC2Role をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 2 月 21 日 22:50 UTC
- 編集日時: 2017 年 2 月 21 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkEnhancedHealth

説明 : Health Monitoring システムの AWS Elastic Beanstalk サービスポリシー

AWSElasticBeanstalkEnhancedHealth は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkEnhancedHealth` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 8 日 23:17 UTC
- 編集日時: 2018 年 4 月 9 日 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkMaintenance

説明: メンテナンス目的でユーザーに代わって リソースを更新するための制限付きアクセス許可を付与する AWS Elastic Beanstalk サービスロールポリシー。

AWSElasticBeanstalkMaintenance は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 1 月 11 日 23:22 UTC
- 編集日時: 2024 年 4 月 29 日 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation>DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:cloudformation:*:*:stack/awseb-*",
      "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
  },
  {
    "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing:DescribeLoadBalancers",
    "Resource" : "*"
  }
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

説明：このポリシーは、AWS Elastic Beanstalk 環境のマネージド更新を実行するために使用される Elastic Beanstalk サービスロール用です。このポリシーは他のユーザーやロールには適用しないでください。このポリシーは、EC2、ECS AutoScaling、Elastic Load Balancing、など、さまざまな AWS のサービスでリソースを作成および管理するための幅広いアクセス許可を付与します CloudFormation。このポリシーでは、それらのサービスで使用可能なすべての IAM ロールを渡すことも許可されます。

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2021 年 3 月 3 日 22:18 UTC
- 編集日時: 2023 年 3 月 23 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```
    ]
  }
}
},
{
  "Sid" : "ReadOnlyPermissions",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:DescribeAccountLimits",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLoadBalancers",
    "autoscaling:DescribeNotificationConfigurations",
    "autoscaling:DescribeScalingActivities",
    "autoscaling:DescribeScheduledActions",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSpotInstanceRequests",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcClassicLink",
    "ec2:DescribeVpcs",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "logs:DescribeLogGroups",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeOrderableDBInstanceOptions",
    "sns:ListSubscriptionsByTopic"
  ],
  "Resource" : [
    "*"
  ]
}
```



```
  },
  {
    "Sid" : "EC2BroadOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions",
      "ec2>DeleteSecurityGroup",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "EC2RunInstancesOperationPermissions",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Sid" : "EC2TerminateInstancesOperationPermissions",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringLike" : {
        "ec2:ResourceTag/aws:cloudformation:stack-id" : [
          "arn:aws:cloudformation:*:*:stack/awseb-e-*",

```

```
        "arn:aws:cloudformation:*:*:stack/eb-*"
    ]
  }
},
{
  "Sid" : "ECSBroadOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:DescribeClusters",
    "ecs:RegisterTaskDefinition"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ECSDeleteClusterOperationPermissions",
  "Effect" : "Allow",
  "Action" : "ecs>DeleteCluster",
  "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
},
{
  "Sid" : "ASGOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteScheduledAction",
    "autoscaling:DetachInstances",
    "autoscaling>DeletePolicy",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:ResumeProcesses",
    "autoscaling:SetDesiredCapacity",
    "autoscaling:SuspendProcesses",
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource" : [
```

```

    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
},
{
  "Sid" : "CFNOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:*"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "ELBOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
    "elasticloadbalancing:ConfigureHealthCheck",
    "elasticloadbalancing>CreateLoadBalancer",
    "elasticloadbalancing>DeleteLoadBalancer",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:DeregisterTargets",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
    "elasticloadbalancing:RegisterTargets"
  ],
  "Resource" : [
    "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/**",
    "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/**"
  ]
},
{
  "Sid" : "CWLogsOperationPermissions",
  "Effect" : "Allow",

```

```
"Action" : [
  "logs:CreateLogGroup",
  "logs>DeleteLogGroup",
  "logs:PutRetentionPolicy"
],
"Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
  "Sid" : "S3ObjectOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
},
{
  "Sid" : "S3BucketOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Sid" : "SNSOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sns:CreateTopic",
    "sns:GetTopicAttributes",
    "sns:SetTopicAttributes",
    "sns:Subscribe"
  ],
  "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
},
}
```

```
{
  "Sid" : "SQSOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:awseb-e-*",
    "arn:aws:sqs:*:*:eb-*"
  ]
},
{
  "Sid" : "CWPutMetricAlarmOperationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricAlarm"
  ],
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:awseb-*",
    "arn:aws:cloudwatch:*:*:alarm:eb-*"
  ]
},
{
  "Sid" : "AllowECSTagResource",
  "Effect" : "Allow",
  "Action" : [
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ecs:CreateAction" : [
        "CreateCluster",
        "RegisterTaskDefinition"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

説明： マネージド更新に制限されたアクセス許可を付与する AWS Elastic Beanstalk サービスロールポリシー。

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 21 日 22:35 UTC
- 編集日時: 2024 年 4 月 29 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
    }
  ]
}
```

```
"Resource" : "*"
},
{
  "Sid" : "ElasticBeanstalkAPIs",
  "Effect" : "Allow",
  "Action" : [
    "elasticbeanstalk:*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ReadOnlyAPIs",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:Describe*",
    "cloudformation:List*",
    "ec2:Describe*",
    "autoscaling:Describe*",
    "elasticloadbalancing:Describe*",
    "logs:DescribeLogGroups",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptionsByTopic",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ASG",
  "Effect" : "Allow",
  "Action" : [
    "autoscaling:AttachInstances",
    "autoscaling:CreateAutoScalingGroup",
    "autoscaling:CreateLaunchConfiguration",
    "autoscaling:CreateOrUpdateTags",
    "autoscaling>DeleteAutoScalingGroup",
    "autoscaling>DeleteLaunchConfiguration",
    "autoscaling>DeleteScheduledAction",
    "autoscaling:DetachInstances",
    "autoscaling:PutNotificationConfiguration",
    "autoscaling:PutScalingPolicy",
    "autoscaling:PutScheduledUpdateGroupAction",
    "autoscaling:ResumeProcesses",
    "autoscaling:SuspendProcesses",
```



```
    "autoscaling:TerminateInstanceInAutoScalingGroup",
    "autoscaling:UpdateAutoScalingGroup"
  ],
  "Resource" : [
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
**",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
    "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
    "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
  ]
},
{
  "Sid" : "CFN",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:CancelUpdateStack",
    "cloudformation>DeleteStack",
    "cloudformation:GetTemplate",
    "cloudformation:UpdateStack",
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/awseb-e-*",
    "arn:aws:cloudformation:*:*:stack/eb-*"
  ]
},
{
  "Sid" : "EC2",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:cloudformation:stack-id" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    }
  }
},
},
```

```
{
  "Sid" : "S3Obj",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectAcl",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionAcl",
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*/**"
},
{
  "Sid" : "S3Bucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy",
    "s3:ListBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
},
{
  "Sid" : "CWL",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
},
{
  "Sid" : "ELB",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:DeRegisterTargets",
    "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
    "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
      "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
      "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
    ]
  },
  {
    "Sid" : "SNS",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic"
    ],
    "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
  },
  {
    "Sid" : "EC2LaunchTemplate",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate",
      "ec2>DeleteLaunchTemplate",
      "ec2:CreateLaunchTemplateVersion",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*"
  },
  {
    "Sid" : "AllowLaunchTemplateRunInstances",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Sid" : "AllowECSTagResource",
    "Effect" : "Allow",
    "Action" : [
      "ecs:TagResource"
    ],
  },
```

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkMulticontainerDocker

説明: Amazon EC2 Container Service を使用してコンテナデプロイタスクを管理するためのアクセス許可をマルチコンテナ Docker 環境のインスタンスに提供します。

AWSElasticBeanstalkMulticontainerDocker は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkMulticontainerDocker をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:15 UTC
- 編集日時: 2023 年 3 月 23 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkReadOnly

説明：読み取り専用アクセス許可を付与します。AWS Elastic Beanstalk アプリケーションに関連するリソースに関する情報を取得するための直接アクセスをオペレーターに明示的に許可します。

AWSElasticBeanstalkReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 22 日 19:02 UTC
- 編集日時: 2021 年 1 月 22 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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


}

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleCore

説明 : AWSElasticBeanstalkRoleCore (Elastic Beanstalk オペレーションロール) ウェブサービス環境のコアオペレーションを許可します。

AWSElasticBeanstalkRoleCore は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleCore をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:48 UTC
- 編集日時 : 2024 年 4 月 30 日 00:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
            "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2>DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
    }
  ]
}
```

```
    "Condition" : {
      "ArnLike" : {
        "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
      }
    }
  },
  {
    "Sid" : "ASG",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:AttachInstances",
      "autoscaling:*LoadBalancer*",
      "autoscaling:*AutoScalingGroup",
      "autoscaling:*LaunchConfiguration",
      "autoscaling:DeleteScheduledAction",
      "autoscaling:DetachInstances",
      "autoscaling:PutNotificationConfiguration",
      "autoscaling:PutScalingPolicy",
      "autoscaling:PutScheduledUpdateGroupAction",
      "autoscaling:ResumeProcesses",
      "autoscaling:SuspendProcesses",
      "autoscaling:*Tags"
    ],
    "Resource" : [
      "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
**",
      "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
    ]
  },
  {
    "Sid" : "ASGPolicy",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DeletePolicy"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "EBSLR",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "S3Obj",
    "Effect" : "Allow",
    "Action" : [
      "s3:Delete*",
      "s3:Get*",
      "s3:Put*"
    ],
    "Resource" : [
      "arn:aws:s3:::elasticbeanstalk-*/*",
      "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
    ]
  },
  {
    "Sid" : "S3Bucket",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetBucket*",
      "s3:ListBucket",
      "s3:PutBucketPolicy"
    ],
    "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
  },
  {
    "Sid" : "CFN",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:GetTemplate",
      "cloudformation:ListStackResources",
      "cloudformation:UpdateStack",
      "cloudformation:ContinueUpdateRollback",
```

```

        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
},
{
    "Sid" : "CloudWatch",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
},
{
    "Sid" : "ELB",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing>Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
    ],
    "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/**",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/**",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/**/*/*"
    ]
},
{
    "Sid" : "ListAPIs",

```

```
"Effect" : "Allow",
"Action" : [
  "autoscaling:Describe*",
  "cloudformation:Describe*",
  "logs:Describe*",
  "ec2:Describe*",
  "ecs:Describe*",
  "ecs:List*",
  "elasticloadbalancing:Describe*",
  "rds:Describe*",
  "sns:List*",
  "iam:List*",
  "acm:Describe*",
  "acm:List*"
],
"Resource" : "*"
},
{
  "Sid" : "AllowPassRole",
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "elasticbeanstalk.amazonaws.com",
        "ec2.amazonaws.com",
        "autoscaling.amazonaws.com",
        "elasticloadbalancing.amazonaws.com",
        "ecs.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleCWL

説明 : (Elastic Beanstalk オペレーションロール) 環境が Amazon CloudWatch Logs ロググループを管理できるようにします。

AWSElasticBeanstalkRoleCWL は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleCWL をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:49 UTC
- 編集日時: 2020 年 6 月 5 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleECS

説明 : (Elastic Beanstalk オペレーションロール) マルチコンテナ Docker 環境が Amazon ECS クラスターを管理できるようにします。

AWSElasticBeanstalkRoleECS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleECS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:47 UTC
- 編集日時: 2023 年 3 月 23 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleRDS

説明 : (Elastic Beanstalk オペレーションロール) 環境が Amazon RDS インスタンスを統合できるようにします。

AWSElasticBeanstalkRoleRDS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC
- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleSNS

説明 : (Elastic Beanstalk オペレーションロール) 環境が Amazon SNS トピック統合を有効にすることを許可します。

AWSElasticBeanstalkRoleSNS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleSNS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:46 UTC
- 編集日時: 2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"br/>  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkRoleWorkerTier

説明 : (Elastic Beanstalk オペレーションロール) ワーカー環境階層が Amazon DynamoDB テーブルと Amazon SQS キューを作成できるようにします。

AWSElasticBeanstalkRoleWorkerTier は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkRoleWorkerTier をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 6 月 5 日 21:43 UTC
- 編集日時: 2020 年 6 月 5 日 21:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkService

説明：このポリシーは非推奨パスにあります。ガイダンスについては、ドキュメントを参照してください。 <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>. AWS Elastic Beanstalk Service ロールポリシーは、ユーザーに代わって リソース (EC2 AutoScaling、S3 CloudFormation、ELB など) を作成および管理するためのアクセス許可を付与します。 EC2, S3 AWSElasticBeanstalkService は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkService をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 4 月 11 日 20:27 UTC
- 編集日時: 2023 年 5 月 10 日 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkServiceRolePolicy

説明：ユーザーに代わってリソース (EC2 AutoScaling、S3、ELB など) を作成および管理するためのアクセス許可を付与する CloudFormation AWS Elastic Beanstalk サービスリンクロールポリシー。EC2, S3

AWSElasticBeanstalkServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 13 日 23:46 UTC
- 編集日時: 2019 年 6 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkWebTier

説明：ウェブサーバー環境のインスタンスに、ログファイルを Amazon S3 にアップロードするためのアクセス権を付与します。

AWSElasticBeanstalkWebTier は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticBeanstalkWebTier をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:08 UTC
- 編集日時: 2020 年 9 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticBeanstalkWorkerTier

説明: ワーカー環境のインスタンスに、ログファイルを Amazon S3 にアップロードするアクセス、Amazon SQS を使用してアプリケーションのジョブキューをモニタリングするアクセス、Amazon DynamoDB を使用してリーダー選択を実行するアクセス、Amazon CloudWatch を使用してヘルスマニタリングのメトリクスを発行するアクセスを提供します。

AWSElasticBeanstalkWorkerTier は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticBeanstalkWorkerTier` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 2 月 8 日 23:12 UTC
- 編集日時: 2020 年 9 月 9 日 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWS Elastic Disaster Recovery Agent Installation Policy

説明：このポリシーでは、外部サーバーを AWS に復旧するために AWS Elastic Disaster Recovery (DRS) で使用されるレプリケーションエージェントをインストールできます AWS。このポリシーを、レプリケーションエージェントのインストールステップで認証情報を提供する AWS IAM ユーザーまたはロールにアタッチします。

AWS Elastic Disaster Recovery Agent Installation Policy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWS Elastic Disaster Recovery Agent Installation Policy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:37 UTC
- 編集日時: 2023 年 11 月 27 日 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryAgentPolicy

説明：このポリシーでは、AWS Elastic Disaster Recovery (DRS) で使用される AWS レプリケーションエージェントを使用して、ソースサーバーを に復旧できます AWS。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryAgentPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryAgentPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:32 UTC
- 編集日時: 2023 年 11 月 27 日 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

ポリシーのバージョニング

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryConsoleFullAccess

説明: このポリシーは、AWS Elastic Disaster Recovery (DRS) のすべてのパブリック APIs へのフルアクセスと、KMS キー、License Manager、Resource Groups、Elastic Load Balancing、IAM、および EC2 情報を読み取るアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSElasticDisasterRecoveryConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:46 UTC
- 編集日時: 2023 年 10 月 16 日 12:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

説明：このポリシーは、AWS Elastic Disaster Recovery (AWS DRS) のすべてのパブリック APIs と、AWS DRS コンソールで使用される他の AWS サービスのすべてのパブリック APIs へのフルアクセスを提供します。このポリシーをユーザーまたはロールにアタッチします。

AWSElasticDisasterRecoveryConsoleFullAccess_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryConsoleFullAccess_v2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 27 日 13:35 UTC
- 編集日時: 2024 年 5 月 19 日 07:38 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryConsoleFullAccess_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:DescribeInstanceState",
  "ec2:DescribeInstanceTypeOfferings",
  "ec2:DescribeLaunchTemplateVersions",
  "ec2:DescribeLaunchTemplates",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSnapshots",
  "ec2:DescribeSubnets",
  "ec2:DescribeVolumes",
  "ec2:GetEbsEncryptionByDefault",
  "ec2:GetEbsDefaultKmsKeyId",
  "ec2:DescribeKeyPairs",
  "ec2:DescribeCapacityReservations",
  "ec2:DescribeHosts"
],
"Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess4",
  "Effect" : "Allow",
  "Action" : "license-manager:ListLicenseConfigurations",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess5",
  "Effect" : "Allow",
  "Action" : "resource-groups:ListGroup",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess6",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing:DescribeLoadBalancers",
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess7",
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:ListInstanceProfiles",
      "iam:ListRoles"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess8",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
      "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "ec2.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      },
      "Bool" : {
        "aws:ViaAWSService" : "true"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess10",
    "Effect" : "Allow",
```

```
"Action" : [
  "ec2:CreateLaunchTemplateVersion",
  "ec2:ModifyLaunchTemplate",
  "ec2>DeleteLaunchTemplateVersions",
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Resource" : "arn:aws:ec2:*:*:launch-template/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  }
}
},
{
  "Sid" : "ConsoleFullAccess11",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess12",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
}
},
{
```

```
"Sid" : "ConsoleFullAccess13",
"Effect" : "Allow",
"Action" : [
  "ec2:StartInstances",
  "ec2:StopInstances",
  "ec2:TerminateInstances",
  "ec2:ModifyInstanceAttribute",
  "ec2:GetConsoleOutput",
  "ec2:GetConsoleScreenshot"
],
"Resource" : "arn:aws:ec2:*:*:instance/*",
"Condition" : {
  "Null" : {
    "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
}
},
{
  "Sid" : "ConsoleFullAccess14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess15",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
```

```
"Resource" : "arn:aws:ec2:*:*:volume/*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
  },
  "Bool" : {
    "aws:ViaAWSService" : "true"
  }
},
{
  "Sid" : "ConsoleFullAccess16",
  "Effect" : "Allow",
  "Action" : "ec2:CreateSecurityGroup",
  "Resource" : "arn:aws:ec2:*:*:vpc/*"
},
{
  "Sid" : "ConsoleFullAccess17",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess18",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSnapshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
```



```
        "aws:ViaAWSService" : "true"
    }
}
},
{
    "Sid" : "ConsoleFullAccess19",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
}
},
{
    "Sid" : "ConsoleFullAccess20",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
        "Null" : {
            "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
            "aws:ViaAWSService" : "true"
        }
    }
}
},
{
    "Sid" : "ConsoleFullAccess21",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
```

```
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
    },
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ConsoleFullAccess22",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AttachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess23",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DetachVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
}
```

```
{
  "Sid" : "ConsoleFullAccess24",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess25",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ],
  "Condition" : {
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess26",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
```

```
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    },
    "Bool" : {
      "aws:ViaAWSService" : "true"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess27",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:launch-template/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate"
      ]
    }
  }
},
{
  "Sid" : "ConsoleFullAccess28",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess29",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets"
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ConsoleFullAccess30",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeInstanceInformation",
      "ssm:DescribeParameters"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess31",
    "Effect" : "Allow",
    "Action" : [
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
      "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
      "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
      "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
      "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : [
          "drs.amazonaws.com"
        ]
      }
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "ConsoleFullAccess32",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
      "aws:CalledVia" : [
        "drs.amazonaws.com"
      ]
    },
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "ConsoleFullAccess33",
  "Effect" : "Allow",
  "Action" : [
    "ssm:ListDocuments",
    "ssm:ListCommandInvocations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConsoleFullAccess34",
  "Effect" : "Allow",
  "Action" : [
    "ssm:GetParameter",
    "ssm:PutParameter"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecoveryService-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "ConsoleFullAccess35",
    "Effect" : "Allow",
    "Action" : [
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/*"
  },
  {
    "Sid" : "ConsoleFullAccess36",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParameters"
    ],
    "Resource" : [
      "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "ssm.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "ConsoleFullAccess37",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetAutomationExecution"
    ],
    "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryConversionServerPolicy

説明：このポリシーは、AWS Elastic Disaster Recovery Conversion サーバーのインスタンスロールにアタッチされます。このポリシーにより、Elastic Disaster Recovery (DRS) コンバージョンサーバー (Elastic Disaster Recovery によって起動される EC2 インスタンス) が DRS サービスと通信できるようになります。このポリシーが適用された IAM ロールは DRS によって DRS 変換サーバーに (EC2 インスタンスプロファイルとして) アタッチされます。DRS 変換サーバーは、必要に応じて DRS によって自動的に起動および終了されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。DRS 変換サーバーは、ユーザーが DRS コンソール、CLI、または API を使用してソースサーバーを復元することを選択したときに、Elastic Disaster Recovery によって使用されます。

AWSElasticDisasterRecoveryConversionServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryConversionServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:42 UTC
- 編集日時: 2023 年 11 月 27 日 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

説明：このポリシーは、AWS Elastic Disaster Recovery (DRS) がクロスアカウントレプリケーションとクロスアカウントフェイルバックをサポートすることを許可します。

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryCrossAccountReplicationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 5 月 14 日 07:16 UTC
- 編集日時: 2024 年 1 月 17 日 13:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWS Elastic Disaster Recovery Ec2 Instance Policy

説明: このポリシーでは、レプリケーションエージェントをインストールして使用することを許可します。AWS レプリケーションエージェントは、AWS Elastic Disaster Recovery (DRS) によって使用され、EC2 (クロスリージョンまたはクロス AZ) で実行されるソースサーバーを復旧します。このポリシーを含む IAM ロールは、EC2 インスタンスに (EC2 インスタンスプロファイルとして) アタッチする必要があります。

AWS Elastic Disaster Recovery Ec2 Instance Policy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElasticDisasterRecoveryEc2InstancePolicy` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 5 月 26 日 12:30 UTC
- 編集日時: 2023 年 11 月 27 日 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

説明： AWSElasticDisasterRecoveryFailbackInstallationPolicy ポリシーを IAM ID にアタッチできます。このポリシーにより、リカバリーインスタンスを元のソースインフラストラクチャにフェールバックするために使用される Elastic Disaster Recovery Failback Client のインストールが可能になります。このポリシーを、Elastic Disaster Recovery Failback Client の実行時に提供した認証情報を持つ IAM ユーザーまたはロールにアタッチしてください。

AWSElasticDisasterRecoveryFailbackInstallationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSElasticDisasterRecoveryFailbackInstallationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 11:02 UTC
- 編集日時: 2023 年 11 月 27 日 13:43 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryFailbackInstallationPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryFailbackPolicy

説明：このポリシーでは、Elastic Disaster Recovery フェイルバッククライアントの使用を許可します。このクライアントは、リカバリインスタンスを元のソースインフラストラクチャにフェイルバックするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryFailbackPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryFailbackPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:41 UTC
- 編集日時: 2023 年 11 月 27 日 12:56 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

説明：このポリシーでは、Amazon SSM および追加のサービスに必要なアクセス許可を使用して、AWS Elastic Disaster Recovery (AWS DRS) で起動後のアクションを実行できます。このポリシーを IAM ロールまたはユーザーにアタッチします。

AWSElasticDisasterRecoveryLaunchActionsPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryLaunchActionsPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 9 月 13 日 07:38 UTC
- 編集日時: 2024 年 5 月 19 日 07:29 UTC
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryLaunchActionsPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    }
  ],
}
```

```
"Sid" : "LaunchActionsPolicy2",
"Effect" : "Allow",
"Action" : [
  "ssm:SendCommand",
  "ssm:StartAutomationExecution"
],
"Resource" : [
  "arn:aws:ssm:*:*:document/*",
  "arn:aws:ssm:*:*:automation-definition/*:*"
],
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "drs.amazonaws.com"
    ]
  },
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "LaunchActionsPolicy3",
  "Effect" : "Allow",
  "Action" : [
    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource" : [
    "arn:aws:ssm:*:*:document/AWS-*",
    "arn:aws:ssm:*:*:document/AWSCodeDeployAgent-*",
    "arn:aws:ssm:*:*:document/AWSConfigRemediation-*",
    "arn:aws:ssm:*:*:document/AWSConformancePacks-*",
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-*",
    "arn:aws:ssm:*:*:document/AWSDistro0Tel-*",
    "arn:aws:ssm:*:*:document/AWSDocs-*",
    "arn:aws:ssm:*:*:document/AWSEC2-*",
    "arn:aws:ssm:*:*:document/AWSEC2Launch-*",
    "arn:aws:ssm:*:*:document/AWSFIS-*",
    "arn:aws:ssm:*:*:document/AWSFleetManager-*",
    "arn:aws:ssm:*:*:document/AWSIncidents-*",
    "arn:aws:ssm:*:*:document/AWSKinesisTap-*",
    "arn:aws:ssm:*:*:document/AWSMigration-*",
    "arn:aws:ssm:*:*:document/AWSNVM-*",
```

```
"arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
"arn:aws:ssm:*::document/AWSObservabilityExporter-*",
"arn:aws:ssm:*::document/AWSPVDriver-*",
"arn:aws:ssm:*::document/AWSQuickSetupType-*",
"arn:aws:ssm:*::document/AWSQuickStarts-*",
"arn:aws:ssm:*::document/AWSRefactorSpaces-*",
"arn:aws:ssm:*::document/AWSResilienceHub-*",
"arn:aws:ssm:*::document/AWSSAP-*",
"arn:aws:ssm:*::document/AWSSAPTools-*",
"arn:aws:ssm:*::document/AWSSQLServer-*",
"arn:aws:ssm:*::document/AWSSSO-*",
"arn:aws:ssm:*::document/AWSSupport-*",
"arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
"arn:aws:ssm:*::document/AmazonCloudWatch-*",
"arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
"arn:aws:ssm:*::document/AmazonECS-*",
"arn:aws:ssm:*::document/AmazonEFSUtils-*",
"arn:aws:ssm:*::document/AmazonEKS-*",
"arn:aws:ssm:*::document/AmazonInspector-*",
"arn:aws:ssm:*::document/AmazonInspector2-*",
"arn:aws:ssm:*::document/AmazonInternal-*",
"arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
"arn:aws:ssm:*::document/AwsVssComponents-*",
"arn:aws:ssm:*::automation-definition/AWS-*:*",
"arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
"arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
"arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
"arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
"arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
"arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
"arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
"arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
"arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
"arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
"arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
"arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
"arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
"arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
"arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
"arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
"arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
"arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
"arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
"arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
```

```
"arn:aws:ssm::*:automation-definition/AWSResilienceHub-*:*",
"arn:aws:ssm::*:automation-definition/AWSSAP-*:*",
"arn:aws:ssm::*:automation-definition/AWSSAPTools-*:*",
"arn:aws:ssm::*:automation-definition/AWSSQLServer-*:*",
"arn:aws:ssm::*:automation-definition/AWSSSO-*:*",
"arn:aws:ssm::*:automation-definition/AWSSupport-*:*",
"arn:aws:ssm::*:automation-definition/AWSSystemsManagerSAP-*:*",
"arn:aws:ssm::*:automation-definition/AmazonCloudWatch-*:*",
"arn:aws:ssm::*:automation-definition/AmazonCloudWatchAgent-*:*",
"arn:aws:ssm::*:automation-definition/AmazonECS-*:*",
"arn:aws:ssm::*:automation-definition/AmazonEFSUtils-*:*",
"arn:aws:ssm::*:automation-definition/AmazonEKS-*:*",
"arn:aws:ssm::*:automation-definition/AmazonInspector-*:*",
"arn:aws:ssm::*:automation-definition/AmazonInspector2-*:*",
"arn:aws:ssm::*:automation-definition/AmazonInternal-*:*",
"arn:aws:ssm::*:automation-definition/AwsEnaNetworkDriver-*:*",
"arn:aws:ssm::*:automation-definition/AwsVssComponents-*:*"
],
"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"  
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

説明：このポリシーは、AWS Elastic Disaster Recovery (DRS) がネットワークレプリケーションをサポートすることを許可します。

AWSElasticDisasterRecoveryNetworkReplicationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryNetworkReplicationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 6 月 11 日 12:36 UTC
- 編集日時: 2024 年 1 月 2 日 13:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryReadOnlyAccess

説明： AWSElasticDisasterRecoveryReadOnlyAccess ポリシーを IAM ID にアタッチできます。このポリシーは、Elastic Disaster Recovery (DRS) のすべての読み取り専用パブリック APIs と、DRS コンソールを完全に読み取り専用にするために必要な他の AWS サービスの一部の読み取り専用 APIs へのアクセス許可を提供します。このポリシーを IAM ユーザーまたはロールにアタッチします。

AWSElasticDisasterRecoveryReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 17 日 10:50 UTC
- 編集日時: 2023 年 11 月 27 日 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]

```

}

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

説明：このポリシーは、Elastic Disaster Recovery のリカバリインスタンスのインスタンスロールにアタッチされます。このポリシーにより、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) Recovery インスタンスが DRS サービスと通信し、元のソースインフラストラクチャにフェイルバックできるようになります。このポリシーが適用された IAM ロールは、Elastic Disaster Recovery によって DRS Recovery インスタンスに (EC2 インスタンスプロファイルとして) アタッチされます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryRecoveryInstancePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryRecoveryInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:20 UTC
- 編集日時: 2023 年 11 月 27 日 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

説明：このポリシーは、Elastic Disaster Recovery レプリケーションサーバーのインスタンスロールにアタッチされます。このポリシーは、Elastic Disaster Recovery によって起動された EC2 インスタンスである Elastic Disaster Recovery (DRS) レプリケーションサーバーが DRS サービスと通

信し、AWS アカウントに EBS スナップショットを作成することを許可します。このポリシーが適用された IAM ロールは Elastic Disaster Recovery によって DRS レプリケーションサーバーに (EC2 インスタンスプロファイルとして) アタッチされます。必要に応じて DRS によって自動的に起動および終了されます。DRS レプリケーションサーバーは、DRS によって管理される復旧プロセスの一環として AWS、外部サーバーからへのデータレプリケーションを容易にするために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryReplicationServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSElasticDisasterRecoveryReplicationServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 11 月 17 日 13:34 UTC
- 編集日時: 2023 年 11 月 27 日 13:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryServiceRolePolicy

説明：このポリシーは、Elastic Disaster Recovery がユーザーに代わって AWS リソースを管理することを許可します。

AWSElasticDisasterRecoveryServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 10:56 UTC
- 編集日時: 2024 年 1 月 17 日 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Sid" : "DRSServiceRolePolicy1",
"Effect" : "Allow",
"Action" : [
  "drs:ListTagsForResource"
],
"Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy2",
  "Effect" : "Allow",
  "Action" : [
    "drs:TagResource"
  ],
  "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
},
{
  "Sid" : "DRSServiceRolePolicy3",
  "Effect" : "Allow",
  "Action" : [
    "drs:CreateRecoveryInstanceForDrs",
    "drs:TagResource"
  ],
  "Resource" : "arn:aws:drs:*:*:source-server/*"
},
{
  "Sid" : "DRSServiceRolePolicy4",
  "Effect" : "Allow",
  "Action" : "iam:GetInstanceProfile",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy5",
  "Effect" : "Allow",
  "Action" : "kms:ListRetirableGrants",
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy6",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
```

```
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVolumeAttribute",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeVpcs",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeManagedPrefixLists",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetManagedPrefixListAssociations"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RegisterImage"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DRSServiceRolePolicy8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeregisterImage"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
```

```
  },
  {
    "Sid" : "DRSServiceRolePolicy9",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy10",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2:DeleteLaunchTemplate",
      "ec2:DeleteLaunchTemplateVersions"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy11",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVolume",
      "ec2:ModifyVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  },
```



```
{
  "Sid" : "DRSServiceRolePolicy12",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy13",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource" : "arn:aws:ec2:*:*:security-group/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy14",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVolume"
  ],
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy15",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:security-group/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy16",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSecurityGroup"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc/*"
  },
  {
    "Sid" : "DRSServiceRolePolicy17",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy18",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
```

```
    "Null" : {
      "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy19",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateSnapshot"
    ],
    "Resource" : "arn:aws:ec2:*:*:snapshot/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy20",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume",
      "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy21",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AttachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  }
}
```

```
  },
  {
    "Sid" : "DRSServiceRolePolicy22",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DetachVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*"
  },
  {
    "Sid" : "DRSServiceRolePolicy23",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
      }
    }
  },
  {
    "Sid" : "DRSServiceRolePolicy24",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ]
  },
  {
    "Sid" : "DRSServiceRolePolicy25",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam:*:*:role/service-role/AWSElasticDisasterRecoveryReplicationServerRole",
```

```
    "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
    "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "ec2.amazonaws.com"
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy26",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateLaunchTemplate",
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy27",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
    }
  }
}
```

```
    }
  }
},
{
  "Sid" : "DRSServiceRolePolicy28",
  "Effect" : "Allow",
  "Action" : "cloudwatch:GetMetricData",
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

説明：このポリシーは、ソースサーバーやジョブなどの AWS Elastic Disaster Recovery (DRS) リソースへの読み取り専用アクセスを許可します。また、変換されたスナップショットを作成し、その EBS スナップショットを特定のアカウントと共有することもできます。

AWSElasticDisasterRecoveryStagingAccountPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryStagingAccountPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 5 月 26 日 09:49 UTC
- 編集日時: 2023 年 11 月 27 日 13:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

説明：このポリシーは、AWS Elastic Disaster Recovery (DRS) によってソースサーバーを別のターゲットアカウントに復旧し、フェイルバックを許可するために使用されます。IAM ユーザーまたはロールにこのポリシーをアタッチすることはおすすめしません。

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElasticDisasterRecoveryStagingAccountPolicy_v2 をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 1 月 5 日 12:11 UTC
- 編集日時: 2023 年 11 月 27 日 13:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:dms:*:*:source-server/*"
    ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

説明 : AWS Elastic Load Balancing コントロールプレーンのサービスリンクロールポリシー - Classic

AWSElasticLoadBalancingClassicServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 19 日 22:36 UTC
- 編集日時: 2019 年 10 月 7 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElasticLoadBalancingServiceRolePolicy

説明: AWS Elastic Load Balancing コントロールプレーンのサービスリンクロールポリシー

AWSElasticLoadBalancingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 19 日 22:19 UTC
- 編集日時: 2021 年 8 月 26 日 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaConvertFullAccess

説明： AWS Management Console および SDK MediaConvert 経由で AWS Elemental へのフルアクセスを提供します。

AWSElementalMediaConvertFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaConvertFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaConvertReadOnly

説明： AWS Management Console および SDK MediaConvert 経由で AWS Elemental への読み取り専用アクセスを提供します。

AWSElementalMediaConvertReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaConvertReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 25 日 19:25 UTC
- 編集日時: 2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaLiveFullAccess

説明： AWS Elemental MediaLive リソースへのフルアクセスを提供します

AWSElementalMediaLiveFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaLiveFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 8 日 17:07 UTC
- 編集日時: 2020 年 7 月 8 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaLiveReadOnly

説明： AWS Elemental MediaLive リソースへの読み取り専用アクセスを提供します

AWSElementalMediaLiveReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaLiveReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 7 月 8 日 16:38 UTC
- 編集日時: 2020 年 7 月 8 日 16:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Effect" : "Allow",
"Action" : [
  "medialive:List*",
  "medialive:Describe*"
],
"Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaPackageFullAccess

説明 : AWS Elemental MediaPackage リソースへのフルアクセスを提供します

AWSElementalMediaPackageFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 29 日 23:39 UTC
- 編集日時: 2017 年 12 月 29 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaPackageReadOnly

説明： AWS Elemental MediaPackage リソースへの読み取り専用アクセスを提供します

AWSElementalMediaPackageReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 12 月 30 日 00:04 UTC

- 編集日時: 2017 年 12 月 30 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaPackageV2FullAccess

説明 : AWS Elemental MediaPackageV2 リソースへのフルアクセスを提供します。

AWSElementalMediaPackageV2FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSElementalMediaPackageV2FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 20:29 UTC
- 編集日時: 2023 年 7 月 25 日 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaPackageV2ReadOnly

説明： AWS Elemental MediaPackageV2 リソースへの読み取り専用アクセスを提供します。

AWSElementalMediaPackageV2ReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaPackageV2ReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 20:31 UTC
- 編集日時: 2023 年 7 月 25 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaStoreFullAccess

説明 : MediaStore APIs

AWSElementalMediaStoreFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaStoreFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 5 日 23:15 UTC
- 編集日時: 2018 年 3 月 5 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
"Statement" : [
  {
    "Action" : [
      "mediastore:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaStoreReadOnly

説明 : MediaStore APIs

AWSElementalMediaStoreReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaStoreReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 8 日 19:48 UTC
- 編集日時: 2018 年 3 月 8 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaTailorFullAccess

説明 : AWS Elemental MediaTailor リソースへのフルアクセスを提供します

AWSElementalMediaTailorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaTailorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 23 日 00:04 UTC
- 編集日時: 2021 年 11 月 23 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSElementalMediaTailorReadOnly

説明： AWS Elemental MediaTailor リソースへの読み取り専用アクセスを提供します

AWSElementalMediaTailorReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSElementalMediaTailorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 23 日 00:05 UTC
- 編集日時: 2021 年 11 月 23 日 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```

```
    "mediatailor:Get*"
  ],
  "Resource" : "*"
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSEnhancedClassicNetworkingMangementPolicy

説明: 拡張クラシックネットワーク管理機能を有効にするポリシー。

AWSEnhancedClassicNetworkingMangementPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 9 月 20 日 17:29 UTC
- 編集日時: 2017 年 9 月 20 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSEntityResolutionConsoleFullAccess

説明：AWS エンティティ解決および関連サービスへのフルアクセスをコンソールに提供します。

AWSEntityResolutionConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEntityResolutionConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 17 日 17:54 UTC

- 編集日時: 2023 年 10 月 16 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSEntityResolutionConsoleReadOnlyAccess

説明： 経由で AWS Entity Resolution への読み取り専用アクセスを提供します AWS Management Console。

AWSEntityResolutionConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSEntityResolutionConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 17 日 18:18 UTC
- 編集日時: 2023 年 8 月 17 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    "Sid" : "EntityResolutionRead",
    "Effect" : "Allow",
    "Action" : [
      "entityresolution:Get*",
      "entityresolution:List*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorEC2Access

説明: このポリシーは、EC2 およびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorEC2Access は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:39 UTC
- 編集日時: 2023 年 11 月 27 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorECSAccess

説明：このポリシーは、ECS およびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorECSAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorECSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:37 UTC
- 編集日時: 2024 年 1 月 25 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorEKSAccess

説明：このポリシーは、EKS およびその他の必要な のサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorEKSAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorEKSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:34 UTC
- 編集日時: 2023 年 11 月 13 日 16:44 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorNetworkAccess

説明: このポリシーは、EC2 ネットワークおよびその他の必要なサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorNetworkAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorNetworkAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:32 UTC
- 編集日時: 2024 年 1 月 25 日 16:07 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorRDSAccess

説明：このポリシーは、RDS およびその他の必要な のサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorRDSAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorRDSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 20:30 UTC
- 編集日時: 2023 年 11 月 13 日 16:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSFaultInjectionSimulatorSSMAccess

説明： このポリシーは、SSM およびその他の必要な のサービスで FIS アクションを実行するためのアクセス許可を Fault Injection Simulator Service に付与します。

AWSFaultInjectionSimulatorSSMAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFaultInjectionSimulatorSSMAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 10 月 26 日 15:33 UTC
- 編集日時: 2023 年 6 月 2 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSFinSpaceServiceRolePolicy

説明: Amazon が使用または管理する AWS のサービス およびリソースへのアクセスを有効にするポリシー FinSpace

AWSFinSpaceServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 12 日 16:42 UTC

- 編集日時：2023 年 12 月 1 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSFMAdminFullAccess

説明: AWS FM 管理者のフルアクセス

AWSFMAdminFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 9 日 18:06 UTC
- 編集日時: 2022 年 10 月 20 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFMAdminReadOnlyAccess

説明 : AWS FM オペレーションのモニタリングを許可する AWS FM 管理者の読み取り専用アクセス

AWSFMAdminReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMAdminReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 5 月 9 日 20:07 UTC
- 編集日時: 2022 年 10 月 31 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSFMMemberReadOnlyAccess

説明： AWS Firewall Manager メンバーアカウントの AWS WAF アクションへの読み取り専用アクセスを提供します

AWSFMMemberReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSFMMemberReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 9 日 21:05 UTC
- 編集日時: 2018 年 5 月 9 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
    },
  ],
}
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSForWordPressPluginPolicy

説明 : AWS For Wordpress プラグインの マネージドポリシー

AWSForWordPressPluginPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSForWordPressPluginPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 30 日 00:27 UTC
- 編集日時: 2020 年 1 月 20 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGitSyncServiceRolePolicy

説明: AWS コード接続が git リポジトリからコンテンツを同期できるようにするポリシー

AWSGitSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 16 日 17:05 UTC
- 編集日時: 2024 年 4 月 26 日 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
    },
  ],
}
```

```
"Resource" : [
  "arn:aws:codestar-connections:*:*:connection/*",
  "arn:aws:codeconnections:*:*:connection/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSGlobalAcceleratorSLRPolicy

説明: EC2 Elastic Network Interface とセキュリティグループを管理するためのアクセス許可を AWS Global Accelerator に付与するポリシー。

AWSGlobalAcceleratorSLRPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 4 月 5 日 19:39 UTC
- 編集日時: 2023 年 9 月 12 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSGlueConsoleFullAccess

説明： 経由で AWS Glue へのフルアクセスを提供します AWS Management Console

AWSGlueConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueConsoleFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 7 月 14 日 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGlueConsoleSageMakerNotebookFullAccess

説明： 経由で AWS Glue へのフルアクセス AWS Management Console と sagemaker ノートブックインスタンスへのアクセスを提供します。

AWSGlueConsoleSageMakerNotebookFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGlueConsoleSageMakerNotebookFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 5 日 17:52 UTC
- 編集日時: 2021 年 7 月 15 日 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AwsGlueDataBrewFullAccessPolicy

説明： DataBrew 経由で AWS Glue へのフルアクセスを提供します AWS Management Console。また、関連サービス (S3、KMS、Glue など) への特定のアクセスも提供します。

AwsGlueDataBrewFullAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueDataBrewFullAccessPolicy をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 11 日 16:51 UTC
- 編集日時: 2022 年 2 月 4 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGlueDataBrewServiceRole

説明: このポリシーは、ユーザーの Glue データカタログに対してアクションを実行するためのアクセス許可を Glue に付与します。また、このポリシーは、Glue が VPC 内のリソースに接続するための ENI を作成できるようにする ec2 アクション、および Glue がレイクフォーメーション内の登録

済みデータにアクセスできるようにするアクセス許可、およびユーザーの cloudwatch にアクセスするアクセス許可も付与します。

AWSGlueDataBrewServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueDataBrewServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 4 日 21:26 UTC
- 編集日時: 2024 年 3 月 20 日 23:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGlueSchemaRegistryFullAccess

説明： AWS Glue Schema Registry Service へのフルアクセスを提供します

AWSGlueSchemaRegistryFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueSchemaRegistryFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 20 日 00:19 UTC
- 編集日時: 2020 年 11 月 20 日 00:19 UTC

- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSGlueSchemaRegistryReadOnlyAccess

説明： AWS Glue Schema Registry Service への読み取り専用アクセスを提供します。

AWSGlueSchemaRegistryReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueSchemaRegistryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 11 月 20 日 00:20 UTC
- 編集日時: 2020 年 11 月 20 日 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSGlueServiceNotebookRole

説明： お客様がノートブックサーバーを管理できるようにする AWS Glue サービスロールのポリシー

AWSGlueServiceNotebookRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueServiceNotebookRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 10 月 9 日 15:59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

ポリシーのバージョニング

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGlueServiceRole

説明： EC2、S3、Cloudwatch Logs などの関連サービスへのアクセスを許可する AWS Glue サービスロールのポリシー EC2, S3

AWSGlueServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGlueServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:37 UTC
- 編集日時: 2023 年 9 月 11 日 16:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AwsGlueSessionUserRestrictedNotebookPolicy

説明：ユーザーに関連付けられているノートブックセッションのみを作成および使用できるようにするアクセス許可を提供します。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

AwsGlueSessionUserRestrictedNotebookPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedNotebookPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 18 日 15:24 UTC
- 編集日時: 2023 年 11 月 22 日 01:32 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

説明：セッションを除くすべての AWS Glue リソースへのフルアクセスを提供します。ユーザーが、ユーザーに関連付けられているノートブックセッションのみを作成して使用できるようにしま

す。このポリシーには、他の AWS サービスの AWS Glue リソースを管理するために Glue が必要とする他のアクセス許可も含まれています。

AwsGlueSessionUserRestrictedNotebookServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedNotebookServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 18 日 15:27 UTC
- 編集日時: 2022 年 4 月 18 日 15:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AwsGlueSessionUserRestrictedPolicy

説明：ユーザーに関連付けられたインタラクティブセッションのみを作成および使用できるようにするアクセス許可を提供します。このポリシーには、ユーザーが制限付き Glue セッションロールを渡すことを明示的に許可するアクセス許可も含まれます。

AwsGlueSessionUserRestrictedPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedPolicy をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 14 日 21:31 UTC
- 編集日時: 2024 年 4 月 29 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    }
  ]
}
```

```
  },
  {
    "Sid" : "AllowGlueActions",
    "Effect" : "Allow",
    "Action" : [
      "glue:RunStatement",
      "glue:GetStatement",
      "glue:ListStatements",
      "glue:CancelStatement",
      "glue:StopSession",
      "glue>DeleteSession",
      "glue:GetSession"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/owner" : "${aws:userid}"
      }
    }
  },
  {
    "Sid" : "AllowListSessions",
    "Effect" : "Allow",
    "Action" : [
      "glue:ListSessions"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "DenyTagActions",
    "Effect" : "Deny",
    "Action" : [
      "glue:TagResource",
      "glue:UntagResource",
      "tag:TagResources",
      "tag:UntagResources"
    ],
    "Resource" : [
      "arn:aws:glue:*:*:session/*"
    ]
  },
```

```
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "owner"
        ]
      }
    },
  ],
  {
    "Sid" : "AllowPassRoleActions",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "glue.amazonaws.com"
        ]
      }
    }
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AwsGlueSessionUserRestrictedServiceRole

説明：セッションを除くすべての AWS Glue リソースへのフルアクセスを提供します。ユーザーは、そのユーザーに関連付けられている対話型セッションのみを作成して使用できるようにします。

このポリシーには、他の AWS サービスの AWS Glue リソースを管理するために Glue が必要とする他のアクセス許可も含まれています。

AwsGlueSessionUserRestrictedServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AwsGlueSessionUserRestrictedServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2022 年 4 月 14 日 21:30 UTC
- 編集日時: 2024 年 4 月 29 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
      ]
    }
  ]
}
```

```
    "arn:aws:glue:*:*:connection/*",
    "arn:aws:glue:*:*:userDefinedFunction/*",
    "arn:aws:glue:*:*:devEndpoint/*",
    "arn:aws:glue:*:*:job/*",
    "arn:aws:glue:*:*:trigger/*",
    "arn:aws:glue:*:*:crawler/*",
    "arn:aws:glue:*:*:workflow/*",
    "arn:aws:glue:*:*:mlTransform/*",
    "arn:aws:glue:*:*:registry/*",
    "arn:aws:glue:*:*:schema/*"
  ]
},
{
  "Sid" : "AllowCompletionActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:StartCompletion",
    "glue:GetCompletion"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:completion/*"
  ]
},
{
  "Sid" : "AllowSessionActions",
  "Effect" : "Allow",
  "Action" : [
    "glue:CreateSession"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/owner" : "${aws:user}"
    },
    "ForAnyValue:StringEquals" : {
      "aws:TagKeys" : [
        "owner"
      ]
    }
  }
},
{
```



```
"Sid" : "AllowStatementActions",
"Effect" : "Allow",
"Action" : [
  "glue:RunStatement",
  "glue:GetStatement",
  "glue:ListStatements",
  "glue:CancelStatement",
  "glue:StopSession",
  "glue>DeleteSession",
  "glue:GetSession"
],
"Resource" : [
  "arn:aws:glue:*:*:session/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/owner" : "${aws:userid}"
  }
}
},
{
  "Sid" : "AllowListSessionsAction",
  "Effect" : "Allow",
  "Action" : [
    "glue:ListSessions"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DenyTagActions",
  "Effect" : "Deny",
  "Action" : [
    "glue:TagResource",
    "glue:UntagResource",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource" : [
    "arn:aws:glue:*:*:session/*"
  ],
  "Condition" : {
    "ForAnyValue:StringEquals" : {
```

```
        "aws:TagKeys" : [
            "owner"
        ]
    }
},
{
    "Sid" : "AllowS3BucketActions",
    "Effect" : "Allow",
    "Action" : [
        "s3:CreateBucket"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*"
    ]
},
{
    "Sid" : "AllowS3ObjectActions",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
    ],
    "Resource" : [
        "arn:aws:s3:::aws-glue-*/**",
        "arn:aws:s3:::*/**aws-glue-*/**"
    ]
},
{
    "Sid" : "AllowS3ObjectCrawlerActions",
    "Effect" : "Allow",
    "Action" : [
        "s3:GetObject"
    ],
    "Resource" : [
        "arn:aws:s3:::crawler-public*"
    ]
},
{
    "Sid" : "AllowLogsActions",
    "Effect" : "Allow",
    "Action" : [
        "logs:CreateLogGroup",
```

```
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:/aws-glue/*"
  ]
},
{
  "Sid" : "AllowTagsActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "aws-glue-service-resource"
      ]
    }
  },
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGrafanaAccountAdministrator

説明 : Amazon Grafana 内で、組織全体のワークスペースを作成および管理するためのアクセスを提供します。

AWSGrafanaAccountAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:20 UTC
- 編集日時: 2022 年 2 月 15 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGrafanaConsoleReadOnlyAccess

説明 : Amazon Grafana での読み取り専用オペレーションへのアクセス。

AWSGrafanaConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSGrafanaConsoleReadOnlyAccess` をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:10 UTC
- 編集日時: 2022 年 2 月 15 日 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGrafanaWorkspacePermissionManagement

説明： AWS Grafana ワークスペースのユーザーおよびグループのアクセス許可を更新する機能のみを提供します。

AWSGrafanaWorkspacePermissionManagement は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaWorkspacePermissionManagement をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 23 日 00:15 UTC
- 編集日時: 2023 年 3 月 15 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGrafanaWorkspacePermissionManagementV2

説明： Amazon Managed Grafana ワークスペースの IAM Identity Center (IdC) ユーザーおよびグループのアクセス許可を更新する機能を提供します。

AWSGrafanaWorkspacePermissionManagementV2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGrafanaWorkspacePermissionManagementV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 1 月 5 日 18:39 UTC
- 編集日時: 2024 年 1 月 5 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGreengrassFullAccess

説明：このポリシーは、AWS Greengrass の設定、管理、デプロイアクションへのフルアクセスを許可します。

AWSGreengrassFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGreengrassFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 5 月 3 日 00:47 UTC
- 編集日時: 2017 年 5 月 3 日 00:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSGreengrassReadOnlyAccess

説明：このポリシーは、AWS Greengrass の設定、管理、デプロイアクションへの読み取り専用アクセスを許可します。

AWSGreengrassReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGreengrassReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 30 日 16:01 UTC
- 編集日時: 2018 年 10 月 30 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGreengrassResourceAccessRolePolicy

説明: Lambda や AWS IoT AWS モノのシャドウなどの関連サービスへのアクセスを許可する AWS Greengrass サービスロールのポリシー。

AWSGreengrassResourceAccessRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGreengrassResourceAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 2 月 14 日 21:17 UTC
- 編集日時: 2018 年 11 月 14 日 00:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

ポリシーのバージョニング

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSGroundStationAgentInstancePolicy

説明： AWS Ground Station エージェントを使用するための Dataflow エンドポイントインスタンスのアクセス許可を提供します

AWSGroundStationAgentInstancePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSGroundStationAgentInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 29 日 15:23 UTC
- 編集日時: 2023 年 3 月 29 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSHealth_EventProcessorServiceRolePolicy

説明 : AWS Health が Health イベントプロセッサ機能を有効にできるようにします。

AWSHealth_EventProcessorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 13 日 19:24 UTC
- 編集日時: 2023 年 1 月 13 日 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSHealthFullAccess

説明 : AWS Health Apis and Notifications と Personal Health Dashboard へのフルアクセスを許可する

AWSHealthFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSHealthFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 6 日 12:30 UTC
- 編集日時: 2020 年 11 月 16 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSHealthImagingFullAccess

説明： AWS Health Imaging サービスへのフルアクセスを提供します。

AWSHealthImagingFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSHealthImagingFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 23:39 UTC
- 編集日時: 2023 年 7 月 25 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSHealthImagingReadOnlyAccess

説明 : AWS Health Imaging サービスへの読み取り専用アクセスを提供します。

AWSHealthImagingReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSHealthImagingReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 7 月 25 日 23:40 UTC
- 編集日時: 2023 年 8 月 1 日 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIAMIdentityCenterAllowListForIdentityContext

説明: IAM Identity Center アイデンティティコンテキストで引き受けられたロールに許可されるアクションのリストを提供します。AWS Security Token Service (AWS STS) は、このポリシーを引き受けられたロールに自動的にアタッチします。ID コンテキストは ProvidedContext として渡されます。

AWSIAMIdentityCenterAllowListForIdentityContext は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIAMIdentityCenterAllowListForIdentityContext をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 8 日 15:21 UTC
- 編集日時: 2024 年 5 月 16 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/
AWSIAMIdentityCenterAllowListForIdentityContext

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena>DeleteNamedQuery",
        "athena>DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
```

```
"elasticmapreduce:DescribeCluster",
"elasticmapreduce:CancelSteps",
"elasticmapreduce:DescribeStep",
"elasticmapreduce:ListSteps",
"glue:GetDatabase",
"glue:GetDatabases",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersions",
"glue:GetPartition",
"glue:GetPartitions",
"glue:BatchGetPartition",
"glue:GetColumnStatisticsForPartition",
"glue:GetColumnStatisticsForTable",
"glue:SearchTables",
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue>DeleteDatabase",
"glue:CreateTable",
"glue>DeleteTable",
"glue:BatchDeleteTable",
"glue:UpdateTable",
"glue:BatchCreatePartition",
"glue:CreatePartition",
"glue>DeletePartition",
"glue:BatchDeletePartition",
"glue:UpdatePartition",
"glue:BatchUpdatePartition",
"glue>DeleteColumnStatisticsForPartition",
"glue>DeleteColumnStatisticsForTable",
"glue:UpdateColumnStatisticsForPartition",
"glue:UpdateColumnStatisticsForTable",
"lakeformation:GetDataAccess",
"s3:GetAccessGrantsInstanceForPrefix",
"s3:GetDataAccess",
"q:StartConversation",
"q:SendMessage",
"q:ListConversations",
"q:GetConversation",
"q:StartTroubleshootingAnalysis",
"q:GetTroubleshootingResults",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateTroubleshootingCommandResult",
"qapps:CreateQApp",
```

```
    "qapps:PredictProblemStatementFromConversation",
    "qapps:PredictQAppFromProblemStatement",
    "qapps:CopyQApp",
    "qapps:GetQApp",
    "qapps:ListQApps",
    "qapps:UpdateQApp",
    "qapps>DeleteQApp",
    "qapps:AssociateQAppWithUser",
    "qapps:DisassociateQAppFromUser",
    "qapps:ImportDocumentToQApp",
    "qapps:ImportDocumentToQAppSession",
    "qapps>CreateLibraryItem",
    "qapps:GetLibraryItem",
    "qapps:UpdateLibraryItem",
    "qapps>CreateLibraryItemReview",
    "qapps:ListLibraryItems",
    "qapps>CreateSubscriptionToken",
    "qapps:StartQAppSession",
    "qapps:StopQAppSession",
    "qbusiness:Chat",
    "qbusiness:ChatSync",
    "qbusiness:ListConversations",
    "qbusiness:ListMessages",
    "qbusiness>DeleteConversation",
    "qbusiness:PutFeedback",
    "sts:SetContext"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIdentitySyncFullAccess

説明： Identity Sync サービスへのフルアクセスを付与します

AWSIdentitySyncFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIdentitySyncFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIdentitySyncReadOnlyAccess

説明： Identity Sync サービスへの読み取り専用アクセス

AWSIdentitySyncReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIdentitySyncReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 3 月 23 日 23:29 UTC
- 編集日時: 2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSImageBuilderFullAccess

説明：すべての AWS Image Builder アクションへのフルアクセスと、関連 AWS サービスへのリソーススコープアクセスを提供します。

AWSImageBuilderFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImageBuilderFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 20 日 18:25 UTC
- 編集日時: 2021 年 4 月 13 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSImageBuilderReadOnlyAccess

説明：すべての AWS Image Builder アクションへの読み取り専用アクセスを提供します。

AWSImageBuilderReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImageBuilderReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 19 日 22:29 UTC
- 編集日時: 2019 年 12 月 19 日 22:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSImportExportFullAccess

説明： で作成されたジョブへの読み取りおよび書き込みアクセスを提供します AWS アカウント。

AWSImportExportFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImportExportFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSImportExportReadOnlyAccess

説明： で作成されたジョブへの読み取り専用アクセスを提供します AWS アカウント。

AWSImportExportReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSImportExportReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

説明： インシデントの管理の一環として他の AWS サービスを呼び出すアクセス許可を Incident Manager に付与します。

AWSIncidentManagerIncidentAccessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIncidentManagerIncidentAccessServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 13 日 00:01 UTC
- 編集日時: 2024 年 2 月 20 日 23:02 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIncidentManagerResolverAccess

説明: このポリシーは、カスタムタイムラインイベントおよび関連項目へのフルアクセスでインシデントを開始、表示、更新するアクセス許可を付与します。インシデントを作成および解決するユーザーにこのポリシー割り当ててください。

AWSIncidentManagerResolverAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIncidentManagerResolverAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 5 月 10 日 06:12 UTC
- 編集日時: 2021 年 5 月 10 日 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIncidentManagerServiceRolePolicy

説明： このポリシーは、ユーザーに代わってインシデントレコードと関連リソースを管理するアクセス許可を Incident Manager に付与します。

AWSIncidentManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 10 日 03:34 UTC
- 編集日時: 2022 年 12 月 5 日 02:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoT1ClickFullAccess

説明： AWS IoT 1-Click へのフルアクセスを提供します。

AWSIoT1ClickFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 11 日 22:10 UTC
- 編集日時: 2018 年 5 月 11 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoT1ClickReadOnlyAccess

説明： AWS IoT 1-Click への読み取り専用アクセスを提供します。

AWSIoT1ClickReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT1ClickReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 11 日 21:49 UTC
- 編集日時: 2018 年 5 月 11 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "iot1click:Describe*",
      "iot1click:Get*",
      "iot1click:List*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTAnalyticsFullAccess

説明：IoT Analytics へのフルアクセスを提供します。

AWSIoTAnalyticsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTAnalyticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 18 日 23:02 UTC
- 編集日時: 2018 年 6 月 18 日 23:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTAnalyticsReadOnlyAccess

説明 : IoT Analytics への読み取り専用アクセスを提供します。

AWSIoTAnalyticsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTAnalyticsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 18 日 21:37 UTC
- 編集日時: 2018 年 6 月 18 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTConfigAccess

説明: このポリシーは、AWS IoT 設定アクションへのフルアクセスを許可します。

AWSIoTConfigAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTConfigAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTConfigReadOnlyAccess

説明：このポリシーは、AWS IoT 設定アクションへの読み取り専用アクセスを許可します。

AWSIoTConfigReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTConfigReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:52 UTC
- 編集日時: 2019 年 9 月 27 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDataAccess

説明：このポリシーは、AWS IoT メッセージングアクションへのフルアクセスを許可します。

AWSIoTDataAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDataAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 27 日 21:51 UTC
- 編集日時: 2021 年 6 月 23 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

説明: IoT_THINGS_TO_THING_GROUP 緩和アクションを実行するための IoT モノグループへの書き込みアクセスと IoT 証明書への読み取りアクセスを提供します

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:55 UTC
- 編集日時: 2019 年 8 月 7 日 17:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderAudit

説明： IoT および関連リソースへの読み取りアクセスを提供します

AWSIoTDeviceDefenderAudit は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderAudit をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 7 月 18 日 21:17 UTC
- 編集日時: 2019 年 11 月 25 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

説明: ENABLE_IOT_LOGGING 緩和アクションを実行するための IoT ログ記録を有効にするためのアクセスを提供します

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

説明： PUBLISH_FINDING_TO_SNS 緩和アクションを実行するための SNS トピックへのメッセージ発行アクセスを提供します

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

説明: REPLACE_DEFAULT_POLICY_VERSION 緩和アクションを実行するための IoT ポリシーへの書き込みアクセスを提供します

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:04 UTC
- 編集日時: 2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

説明： UPDATE_CA_CERTIFICATE 緩和アクションを実行するための IoT CA 証明書への書き込みアクセスを提供します

AWSIoTDeviceDefenderUpdateCACertMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTDeviceDefenderUpdateCACertMitigationAction` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:05 UTC
- 編集日時: 2019 年 8 月 7 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

説明： UPDATE_DEVICE_CERTIFICATE 緩和アクションを実行するための IoT 証明書への書き込みアクセスを提供します

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 8 月 7 日 17:06 UTC
- 編集日時: 2019 年 8 月 7 日 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

説明: AWS IoT Device Tester が IoT、S3、IAM IoT などのサービスへのアクセスを許可して FreeRTOS 認定スイートを実行できるようにします

AWSIoTDeviceTesterForFreeRTOSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceTesterForFreeRTOSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 2 月 12 日 20:33 UTC
- 編集日時: 2023 年 8 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:::afri-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:::afri-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"
        ]
      }
    }
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTDeviceTesterForGreengrassFullAccess

説明: Lambda、AWS IoT、API Gateway、IAM などの関連サービスへのアクセスを許可することで、IoT Device Tester が AWS Greengrass 認定スイートを実行できるようにします

AWSIoTDeviceTesterForGreengrassFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTDeviceTesterForGreengrassFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2020 年 2 月 20 日 21:21 UTC
- 編集日時: 2020 年 6 月 25 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTEventsFullAccess

説明：IoT イベントへのフルアクセスを提供します。

AWSIoTEventsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTEventsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 10 日 22:51 UTC
- 編集日時: 2019 年 1 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTEventsReadOnlyAccess

説明：IoT イベントへの読み取り専用アクセスを提供します。

AWSIoTEventsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTEventsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 10 日 22:50 UTC
- 編集日時: 2019 年 9 月 23 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoT FleetHubFederationAccess

説明 : IoT Fleet Hub アプリケーションのフェデレーションアクセス

AWSIoT FleetHubFederationAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoT FleetHubFederationAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 15 日 08:08 UTC
- 編集日時: 2022 年 4 月 4 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoT FleetwiseServiceRolePolicy

説明: 補助機能のために が使用または管理する AWS リソースと metaData AWSIoT Fleetwise にアクセス許可を付与します

AWSIoT FleetwiseServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 9 月 21 日 23:27 UTC
- 編集日時: 2022 年 9 月 21 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoT FleetwiseServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTFullAccess

説明: このポリシーは、AWS IoT 設定およびメッセージングアクションへのフルアクセスを許可します。

AWSIoTFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 8 日 15:19 UTC
- 編集日時: 2022 年 5 月 19 日 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTLogging

説明： Amazon CloudWatch Log グループの作成とグループへのログのストリーミングを許可します

AWSIoTLogging は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTLogging をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:17 UTC
- 編集日時: 2015 年 10 月 8 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "logs:CreateLogGroup",
  "logs:CreateLogStream",
  "logs:PutLogEvents",
  "logs:PutMetricFilter",
  "logs:PutRetentionPolicy",
  "logs:GetLogEvents",
  "logs>DeleteLogStream"
],
"Resource" : [
  "*"
]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTOTAUpdate

説明 : AWS IoT ジョブを作成し、AWS コード署名者ジョブを記述するためのアクセスを許可します

AWSIoTOTAUpdate は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTOTAUpdate をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 20 日 20:36 UTC
- 編集日時: 2017 年 12 月 20 日 20:36 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTRoboRunnerFullAccess

説明：このポリシーは、IoT AWS へのフルアクセスを許可するアクセス許可を付与します RoboRunner。

AWSIoTRoboRunnerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSIoTRoboRunnerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 03:54 UTC
- 編集日時: 2023 年 2 月 23 日 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTRoboRunnerReadOnly

説明： このポリシーは、AWS IoT への読み取り専用アクセスを許可するアクセス許可を付与します RoboRunner。

AWSIoTRoboRunnerReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTRoboRunnerReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 03:43 UTC
- 編集日時: 2022 年 11 月 16 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTRoboRunnerServiceRolePolicy

説明： お客様に代わって関連する AWS リソースを管理 AWS IoT RoboRunner できるようにします。

AWSIoTRoboRunnerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 2 月 21 日 16:56 UTC
- 編集日時: 2023 年 2 月 21 日 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTRuleActions

説明： AWS IoT ルールアクションでサポートされているすべての AWS サービスへのアクセスを許可します

AWSIoTRuleActions は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTRuleActions をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 10 月 8 日 15:14 UTC
- 編集日時: 2018 年 1 月 16 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTSiteWiseConsoleFullAccess

説明： を使用して manage AWS IoT SiteWise へのフルアクセスを提供します AWS Management Console。このポリシーは、AWS IoT SiteWise (AWS IoT Analytics など) で使用されるデータストアの作成と一覧表示、AWS IoT Greengrass リソースの一覧表示と表示、AWS Secrets Manager シークレットの一覧表示と変更、AWS IoT モノのシャドウの取得、特定のタグを持つリソースの一覧表示、AWS IoT SiteWise のサービスにリンクされたロールの作成と使用のためのアクセスも許可することに注意してください。

AWSIoTSiteWiseConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseConsoleFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 5 月 31 日 21:37 UTC
- 編集日時: 2019 年 5 月 31 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/AWSIoTServiceRoleForIoTSiteWise*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : "iotsitewise.amazonaws.com"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTSiteWiseFullAccess

説明 : IoT へのフルアクセスを提供します SiteWise。

AWSIoTSiteWiseFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 12 月 4 日 20:53 UTC

- 編集日時: 2018 年 12 月 4 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTSiteWiseMonitorPortalAccess

説明: このポリシーは、AWS IoT SiteWise アセットとアセットデータへのアクセス、AWS IoT SiteWise Monitor リソースの作成、および AWS SSO ユーザーのリストを取得するアクセス許可を付与します。

AWSIoTSiteWiseMonitorPortalAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseMonitorPortalAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 5 月 19 日 20:01 UTC
- 編集日時: 2020 年 5 月 19 日 20:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

説明: このロールは AWS IoT SiteWise アセットとアセットプロパティにアクセスするためのアクセス許可を AWS IoT SiteWise モニターに付与し、AWS IoT SiteWise ポータルを通じて AWS IoT SiteWise プロジェクト、ダッシュボード、アクセスポリシーを作成します。

AWSIoTSiteWiseMonitorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 14 日 00:59 UTC
- 編集日時: 2019 年 12 月 13 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTSiteWiseReadOnlyAccess

説明：IoT への読み取り専用アクセスを提供します SiteWise。

AWSIoTSiteWiseReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTSiteWiseReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 12 月 4 日 20:55 UTC
- 編集日時: 2022 年 9 月 16 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTThingsRegistration

説明：このポリシーでは、ユーザーは AWS IoT StartThingRegistrationTask API を使用してモノを一括登録できます。

AWSIoTThingsRegistration は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTThingsRegistration をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 12 月 1 日 20:21 UTC
- 編集日時: 2020 年 10 月 5 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTtwinMakerServiceRolePolicy

説明: 他の AWS サービスを呼び出し、ユーザーに代わってリソースを同期することを AWS IoT TwinMaker に許可します。

AWSIoTtwinMakerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 13 日 18:59 UTC
- 編集日時: 2023 年 11 月 13 日 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessDataAccess

説明：関連付けられた ID データの AWS IoT Wireless デバイスへのアクセスを許可します。

AWSIoTWirelessDataAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessDataAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:31 UTC
- 編集日時: 2020 年 12 月 15 日 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessFullAccess

説明： 関連付けられた ID に、すべての AWS IoT Wireless オペレーションへのフルアクセスを許可します。

AWSIoTWirelessFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:27 UTC
- 編集日時: 2020 年 12 月 15 日 15:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessFullPublishAccess

説明： IoT Wireless に、ユーザーに代わって IoT ルールエンジンに発行するためのフルアクセスを提供します。

AWSIoTWirelessFullPublishAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessFullPublishAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:29 UTC
- 編集日時: 2020 年 12 月 15 日 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ]
    }
  ]
}
```



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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessGatewayCertManager

説明：関連付けられた ID アクセスが IoT 証明書を作成、一覧表示、および記述できるようにします。

AWSIoTWirelessGatewayCertManager は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessGatewayCertManager をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:30 UTC
- 編集日時: 2020 年 12 月 15 日 15:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessLogging

説明： 関連付けられた ID が Amazon CloudWatch Logs グループを作成し、グループにログをストリーミングできるようにします。

AWSIoTWirelessLogging は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessLogging をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:32 UTC
- 編集日時: 2020 年 12 月 15 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIoTWirelessReadOnlyAccess

説明： 関連付けられた ID に AWS IoT ワイヤレスへの読み取り専用アクセスを許可します。

AWSIoTWirelessReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIoTWirelessReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 15 日 15:28 UTC
- 編集日時: 2020 年 12 月 15 日 15:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIPAMServiceRolePolicy

説明： VPC IP Address Manager が VPC リソースにアクセスし、ユーザーに代わって AWS Organizations と統合できるようにします。

AWSIPAMServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 30 日 19:08 UTC
- 編集日時: 2023 年 11 月 8 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIQContractServiceRolePolicy

説明： AWS IQ が顧客に代わって支払いリクエストを実行するために使用されます

AWSIQContractServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 22 日 19:28 UTC
- 編集日時: 2019 年 8 月 22 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSIQFullAccess

説明： AWS IQ へのフルアクセスを提供します

AWSIQFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSIQFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 4 月 4 日 23:13 UTC

- 編集日時: 2019 年 9 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSIQPermissionServiceRolePolicy

説明 : AWS IQ が AWS IQ の専門家が引き受けるロールを管理できるようにします。

AWSIQPermissionServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 22 日 19:36 UTC
- 編集日時: 2019 年 8 月 22 日 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

説明 : AWS KMS カスタムキーストアに必要な AWS サービスとリソースへのアクセスを有効にする

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 20:10 UTC
- 編集日時: 2023 年 11 月 10 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

説明 : AWS KMS がマルチリージョンキーの共有プロパティを同期できるようにします。

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 15:37 UTC
- 編集日時: 2021 年 6 月 16 日 15:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSKeyManagementServicePowerUser

説明 : AWS Key Management Service (KMS) へのアクセスを提供します。

AWSKeyManagementServicePowerUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSKeyManagementServicePowerUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 3 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLakeFormationCrossAccountManager

説明： Lake Formation 経由で Glue リソースへのクロスアカウントアクセスを提供します。組織やリソースアクセスマネージャーなど、他の必要なサービスへの読み取りアクセスも付与します

AWSLakeFormationCrossAccountManager は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLakeFormationCrossAccountManager をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 4 日 20:59 UTC
- 編集日時: 2024 年 3 月 22 日 18:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "AllowCreateResourceShare",
    "Effect" : "Allow",
    "Action" : [
      "ram:CreateResourceShare"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLikeIfExists" : {
        "ram:RequestedResourceType" : [
          "glue:Table",
          "glue:Database",
          "glue:Catalog"
        ]
      }
    }
  },
  {
    "Sid" : "AllowManageResourceShare",
    "Effect" : "Allow",
    "Action" : [
      "ram:UpdateResourceShare",
      "ram>DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:GetResourceShares"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ram:ResourceShareName" : [
          "LakeFormation*"
        ]
      }
    }
  },
  {
    "Sid" : "AllowManageResourceSharePermissions",
    "Effect" : "Allow",
    "Action" : [
      "ram:AssociateResourceSharePermission"
    ],
  },

```

```
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "ram:PermissionArn" : [
      "arn:aws:ram::aws:permission/AWSRAMLFEabled*"
    ]
  }
},
{
  "Sid" : "AllowXAcctManagerPermissions",
  "Effect" : "Allow",
  "Action" : [
    "glue:PutResourcePolicy",
    "glue>DeleteResourcePolicy",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "ram:Get*",
    "ram:List*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AllowOrganizationsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListRoots",
    "organizations:ListAccountsForParent",
    "organizations:ListOrganizationalUnitsForParent"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLakeFormationDataAdmin

説明： データレイクを管理するための AWS Lake Formation および AWS Glue などの関連サービスへの管理アクセスを付与します

AWSLakeFormationDataAdmin は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLakeFormationDataAdmin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 8 月 8 日 17:33 UTC
- 編集日時: 2024 年 3 月 22 日 18:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
```

```
"glue:CreateDatabase",
"glue:UpdateDatabase",
"glue>DeleteDatabase",
"glue:GetConnections",
"glue:SearchTables",
"glue:GetTable",
"glue:CreateTable",
"glue:UpdateTable",
"glue>DeleteTable",
"glue:GetTableVersions",
"glue:GetPartitions",
"glue:GetTables",
"glue:ListWorkflows",
"glue:BatchGetWorkflows",
"glue>DeleteWorkflow",
"glue:GetWorkflowRuns",
"glue:StartWorkflowRun",
"glue:GetWorkflow",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"s3:GetBucketAcl",
"iam:ListUsers",
"iam:ListRoles",
"iam:GetRole",
"iam:GetRolePolicy"
],
"Resource" : "*"
},
{
  "Sid" : "AWSLakeFormationDataAdminDeny",
  "Effect" : "Deny",
  "Action" : [
    "lakeformation:PutDataLakeSettings"
  ],
  "Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambda_FullAccess

説明： AWS Lambda サービス、 AWS Lambda コンソール機能、 およびその他の関連 AWS サービスへのフルアクセスを許可します。

AWSLambda_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambda_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 17 日 21:14 UTC
- 編集日時: 2020 年 11 月 17 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambda_ReadOnlyAccess

説明： AWS Lambda サービス、AWS Lambda コンソール機能、およびその他の関連 AWS サービスへの読み取り専用アクセスを許可します。

AWSLambda_ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambda_ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 17 日 21:10 UTC
- 編集日時: 2023 年 7 月 27 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaBasicExecutionRole

説明： CloudWatch ログへの書き込みアクセス許可を提供します。

AWSLambdaBasicExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaBasicExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:03 UTC
- 編集日時: 2015 年 4 月 9 日 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaDynamoDBExecutionRole

説明 : DynamoDB ストリームへのリストと読み取りアクセス、および CloudWatch ログへの書き込みアクセス許可を提供します。

AWSLambdaDynamoDBExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaDynamoDBExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:09 UTC
- 編集日時: 2015 年 4 月 9 日 15:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaENIManagementAccess

説明 : VPC 対応 Lambda 関数で使用される ENIs (作成、説明、削除) を管理するための Lambda 関数の最小限のアクセス許可を提供します。

AWSLambdaENIManagementAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaENIManagementAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 6 日 00:37 UTC
- 編集日時: 2020 年 10 月 1 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaExecute

説明 : S3 への Put、Get アクセス、および CloudWatch Logs へのフルアクセスを提供します。

AWSLambdaExecute は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaExecute をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaFullAccess

説明：このポリシーは非推奨パスにあります。ガイダンスについては、<https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html> を参照してください。Lambda、S3、DynamoDB、CloudWatch メトリクス、ログへのフルアクセスを提供します。

AWSLambdaFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2017 年 11 月 27 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaInvocation-DynamoDB

説明： DynamoDB Streams への読み取りアクセスを提供します。

AWSLambdaInvocation-DynamoDB は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaInvocation-DynamoDB をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaKinesisExecutionRole

説明： Kinesis ストリームへのリストと読み取りアクセスと、 CloudWatch ログへの書き込みアクセス許可を提供します。

AWSLambdaKinesisExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSLambdaKinesisExecutionRole` をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 4 月 9 日 15:14 UTC
- 編集日時: 2018 年 11 月 19 日 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaMSKExecutionRole

説明: VPC 内の MSK クラスターにアクセスし、VPC 内の ENIs (作成、説明、削除) を管理し、CloudWatch ログに許可を書き込むために必要な許可を提供します。

AWSLambdaMSKExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaMSKExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 17:35 UTC
- 編集日時: 2022 年 8 月 2 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaReplicator

説明：リージョン間で関数をレプリケートするために必要なアクセス許可を Lambda レプリケーターに付与します

AWSLambdaReplicator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 5 月 23 日 17:53 UTC
- 編集日時: 2017 年 12 月 8 日 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaRole

説明：AWS Lambda サービスロールのデフォルトポリシー。

AWSLambdaRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaSQSQueueExecutionRole

説明：受信メッセージ、削除メッセージ、SQS キューへの読み取り属性アクセス、CloudWatch ログへの書き込みアクセス許可を提供します。

AWSLambdaSQSQueueExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaSQSQueueExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 14 日 21:50 UTC
- 編集日時: 2018 年 6 月 14 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLambdaVPCAccessExecutionRole

説明 : VPC 内のリソースへのアクセス中に Lambda 関数が実行する最小限のアクセス許可を提供します。ネットワークインターフェイスの作成、説明、削除、および CloudWatch Logs への書き込みアクセス許可。

AWSLambdaVPCAccessExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLambdaVPCAccessExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 2 月 11 日 23:15 UTC
- 編集日時: 2024 年 1 月 5 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerConsumptionPolicy

説明：ユーザーが使用権限を持っているライセンスで消費するために必要な AWS License Manager API アクションへのアクセスを許可するアクセス許可を提供します。

AWSLicenseManagerConsumptionPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSLicenseManagerConsumptionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 8 月 11 日 23:18 UTC
- 編集日時: 2021 年 8 月 11 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

説明： AWS License Manager Linux Subscriptions Service がユーザーに代わってリソースを管理できるようにします。

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 20 日 18:54 UTC
- 編集日時: 2022 年 12 月 20 日 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerMasterAccountRolePolicy

説明 : AWS License Manager サービスマスターアカウントロールポリシー

AWSLicenseManagerMasterAccountRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:03 UTC
- 編集日時: 2022 年 5 月 31 日 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerMemberAccountRolePolicy

説明 : AWS License Manager サービスメンバーアカウントロールポリシー

AWSLicenseManagerMemberAccountRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:04 UTC
- 編集日時: 2019 年 11 月 15 日 22:09 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerServiceRolePolicy

説明 : AWS License Manager サービスのデフォルトロールポリシー

AWSLicenseManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:02 UTC
- 編集日時: 2021 年 7 月 30 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

説明：AWS License Manager User Subscriptions Service がユーザーに代わってリソースを管理できるようにします。

AWSLicenseManagerUserSubscriptionsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 30 日 01:17 UTC
- 編集日時: 2022 年 11 月 21 日 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSM2ServicePolicy

説明： AWS M2 がユーザーに代わって AWS リソースを管理できるようにします。

AWSM2ServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2022 年 6 月 7 日 20:26 UTC
- 編集日時: 2022 年 6 月 7 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSManagedServices_ContactsServiceRolePolicy

説明 : AWS Managed Services が AWS リソースのタグの値を読み取ることを許可する

AWSManagedServices_ContactsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 23 日 17:07 UTC
- 編集日時: 2023 年 3 月 23 日 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

説明 : AWS マネージドサービス - 検出コントロールインフラストラクチャを管理するためのポリシー

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 19 日 23:11 UTC
- 編集日時: 2022 年 12 月 19 日 23:11 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSManagedServices_EventsServiceRolePolicy

説明 : AMS イベントプロセッサ機能を有効にするマネージド AWS サービスポリシー。

AWSManagedServices_EventsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 2 月 7 日 18:41 UTC
- 編集日時: 2023 年 2 月 7 日 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSManagedServicesDeploymentToolkitPolicy

説明： AWS Managed Services がユーザーに代わってデプロイツールキットを管理できるようにします。

AWSManagedServicesDeploymentToolkitPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 9 日 18:33 UTC
- 編集日時: 2024 年 4 月 4 日 20:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
```

```
    "s3:PutBucketAcl",
    "s3:PutBucketLogging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketTagging",
    "s3:PutBucketVersioning",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
},
{
  "Sid" : "AMSCDKToolkitCloudFormationPermissions",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateChangeSet",
    "cloudformation>DeleteChangeSet",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeChangeSet",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:GetTemplate",
    "cloudformation:GetTemplateSummary",
    "cloudformation:TagResource",
    "cloudformation:UntagResource",
    "cloudformation:UpdateTerminationProtection"
  ],
  "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
},
{
  "Sid" : "AMSCDKToolkitECRPermissions",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:CreateRepository",
    "ecr>DeleteLifecyclePolicy",
    "ecr>DeleteRepository",
    "ecr>DeleteRepositoryPolicy",
    "ecr:DescribeRepositories",
    "ecr:GetLifecyclePolicy",
    "ecr:ListTagsForResource",
```

```
    "ecr:PutImageScanningConfiguration",
    "ecr:PutImageTagMutability",
    "ecr:PutLifecyclePolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceAmiIngestion

説明 : AWS Marketplace が Amazon マシンイメージ (AMIs) をコピーして に一覧表示することを許可する AWS Marketplace

AWSMarketplaceAmiIngestion は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceAmiIngestion をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 25 日 20:55 UTC
- 編集日時: 2020 年 9 月 25 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceDeploymentServiceRolePolicy

説明： AWS Marketplace でサブスクライブする製品の販売者デプロイパラメータの作成と管理を に許可します AWS Marketplace。

AWSMarketplaceDeploymentServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 23:34 UTC
- 編集日時: 2023 年 11 月 15 日 23:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  ]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceFullAccess

説明: AWS Marketplace ソフトウェアのサブスクライブとサブスクライブ解除を行う機能を提供し、ユーザーが Marketplace の「ソフトウェア」ページから Marketplace ソフトウェアインスタンスを管理できるようにし、EC2 への管理アクセスを提供します。

AWSMarketplaceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 11 日 17:21 UTC
- 編集日時: 2022 年 3 月 4 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceGetEntitlements

説明： AWS Marketplace エンタイトルメントへの読み取りアクセスを提供します

AWSMarketplaceGetEntitlements は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceGetEntitlements をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 3 月 27 日 19:37 UTC
- 編集日時: 2024 年 4 月 5 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceImageBuildFullAccess

説明：AWS Marketplace プライベートイメージ構築機能へのフルアクセスを提供します。プライベートイメージを作成することに加えて、イメージにタグを追加したり、EC2 インスタンスを起動および終了したりする許可も付与されます。

AWSMarketplaceImageBuildFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceImageBuildFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 7 月 31 日 23:29 UTC
- 編集日時: 2022 年 3 月 4 日 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

説明： ライセンス管理 AWS Marketplace のために が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします。

AWSMarketplaceLicenseManagementServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 3 日 08:33 UTC
- 編集日時: 2020 年 12 月 3 日 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceManageSubscriptions

説明： AWS Marketplace ソフトウェアのサブスクライブとサブスクライブ解除の機能を提供します。

AWSMarketplaceManageSubscriptions は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceManageSubscriptions をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC

- 編集日時: 2023 年 1 月 19 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceMeteringFullAccess

説明： Metering AWS Marketplace へのフルアクセスを提供します。

AWSMarketplaceMeteringFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceMeteringFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 3 月 17 日 22:39 UTC
- 編集日時: 2016 年 3 月 17 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceMeteringRegisterUsage

説明： AWS Marketplace Metering Service を通じてリソースを登録し、使用状況を追跡するアクセス許可を提供します。

AWSMarketplaceMeteringRegisterUsage は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceMeteringRegisterUsage をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 21 日 01:17 UTC

- 編集日時: 2019 年 11 月 21 日 01:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceProcurementSystemAdminFullAccess

説明 : AWS Marketplace eProcurement 統合のすべての管理アクションへのフルアクセスを提供します。

AWSMarketplaceProcurementSystemAdminFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceProcurementSystemAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 25 日 13:07 UTC
- 編集日時: 2019 年 6 月 25 日 13:07 UTC
- ARN: arn:aws:iam::aws:policy/
AWSMarketplaceProcurementSystemAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

説明 : AWS Marketplace サービスから発注書管理へのアクセスを有効にします。

AWSMarketplacePurchaseOrdersServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 27 日 15:12 UTC
- 編集日時: 2021 年 10 月 27 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceRead-only

説明： AWS Marketplace サブスクリプションを確認する機能を提供します

AWSMarketplaceRead-only は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceRead-only をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 1 月 19 日 23:30 UTC

- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

説明：再販売承認 AWS Marketplace のために が使用または管理する AWS のサービス および リソースへのアクセスを有効にします。

AWSMarketplaceResaleAuthorizationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 3 月 5 日 18:47 UTC
- 編集日時: 2024 年 3 月 5 日 18:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceSellerFullAccess

説明 : AWS Marketplace および AMI 管理などの他の AWS サービスに対するすべての販売者オペレーションへのフルアクセスを提供します。

AWSMarketplaceSellerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceSellerFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 20:40 UTC
- 編集日時: 2024 年 3 月 15 日 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceSellerProductsFullAccess

説明：販売者に AWS Marketplace Management Products ページや AMI 管理などのその他の AWS サービスへのフルアクセスを提供します。

AWSMarketplaceSellerProductsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMarketplaceSellerProductsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 21:06 UTC
- 編集日時: 2023 年 7 月 18 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMarketplaceSellerProductsReadOnly

説明：販売者に AWS Marketplace Management Products ページへの読み取り専用アクセスを提供します。

AWSMarketplaceSellerProductsReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSMarketplaceSellerProductsReadOnly` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 2 日 21:40 UTC
- 編集日時: 2022 年 11 月 19 日 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMediaConnectServicePolicy

説明：が使用または管理する AWS のサービス およびリソースへのアクセスを有効にするデフォルトのポリシー MediaConnect。

AWSMediaConnectServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 3 日 22:11 UTC
- 編集日時: 2023 年 4 月 3 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMediaTailorServiceRolePolicy

説明： が使用または管理する AWS リソースへのアクセスを有効にする MediaTailor

AWSMediaTailorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 17 日 22:27 UTC
- 編集日時: 2021 年 9 月 17 日 22:27 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubDiscoveryAccess

説明：ポリシーでは AWSMigrationHubService 、 が顧客 AWSApplicationDiscoveryService に代わって を呼び出すことができます。

AWSMigrationHubDiscoveryAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubDiscoveryAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:30 UTC
- 編集日時: 2020 年 8 月 6 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubDMSAccess

説明: Database Migration Service が Migration Hub を呼び出すためにお客様のアカウントでロールを引き受けるためのポリシー

AWSMigrationHubDMSAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubDMSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 14:00 UTC
- 編集日時: 2019 年 10 月 7 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubFullAccess

説明: Migration Hub Service への顧客アクセスを提供する管理ポリシー

AWSMigrationHubFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 8 月 14 日 14:02 UTC
- 編集日時: 2019 年 6 月 19 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubOrchestratorConsoleFullAccess

説明： AWS Migration Hub、 AWS Application Discovery Service、 Amazon Simple Storage Service、 AWS Secrets Manager への制限付きアクセスを提供します。このポリシーは、 AWS Migration Hub Orchestrator サービスへのフルアクセスも付与します。

AWSMigrationHubOrchestratorConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 20 日 02:26 UTC
- 編集日時: 2023 年 12 月 5 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

説明: このポリシーは、S3 からスクリプトをダウンロードしてインスタンスをオーケストレーションし、EC2 インスタンス内でシークレット値を取得するために、SAP および MGN に移行した サービスのインスタンスにアタッチする必要があります。

AWSMigrationHubOrchestratorInstanceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 20 日 02:43 UTC
- 編集日時: 2022 年 4 月 20 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/
AWSMigrationHubOrchestratorInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubOrchestratorPlugin

説明: AWS Migration Hub Orchestrator の Amazon Simple Storage Service、AWS Secrets Manager、プラグイン関連のアクションへの制限付きアクセスを提供します。

AWSMigrationHubOrchestratorPlugin は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubOrchestratorPlugin をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 4 月 20 日 02:25 UTC
- 編集日時: 2022 年 4 月 20 日 02:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
```


このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 4 月 20 日 02:24 UTC
- 編集日時: 2024 年 3 月 4 日 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

説明： ネットワークブリッジのない環境を使用する場合に必要な AWS Transit Gateway および EC2 セキュリティグループを除く AWS Migration Hub リファクタリングスペースおよびその他の AWS 関連サービスへのフルアクセスを許可します。このポリシーでは、タグに基づいてスコープダウンできるため、AWS Lambda と AWS Resource Access Manager に必要なアクセス許可も除外されます。

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 4 月 3 日 20:09 UTC
- 編集日時: 2024 年 4 月 11 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
        "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
}
},
{
    "Sid" : "VpcEndpointServiceConfigurationDelete",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
    "Resource" : "*",
    "Condition" : {
        "Null" : {
            "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
    }
},
{
    "Sid" : "ELBLoadBalancerCreate",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
    "Condition" : {
        "Null" : {
            "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
    }
},
{
    "Sid" : "ELBDescribe",
    "Effect" : "Allow",
    "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
},
{
    "Sid" : "ELBModify",
```

```

    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:RegisterTargets",
      "elasticloadbalancing:CreateLoadBalancerListeners",
      "elasticloadbalancing:CreateListener",
      "elasticloadbalancing>DeleteListener",
      "elasticloadbalancing>DeleteTargetGroup"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/refactor-spaces:route-id" : [
          "*"
        ]
      }
    }
  },
  {
    "Sid" : "ELBLoadBalancerDelete",
    "Effect" : "Allow",
    "Action" : "elasticloadbalancing>DeleteLoadBalancer",
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
  },
  {
    "Sid" : "ELBListenerCreate",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateListener"
    ],
    "Resource" : [
      "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
      "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Sid" : "ELBListenerDelete",
    "Effect" : "Allow",

```

```
    "Action" : "elasticloadbalancing:DeleteListener",
    "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  },
  {
    "Sid" : "ELBTargetGroupModify",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DeleteTargetGroup",
      "elasticloadbalancing:RegisterTargets"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
  },
  {
    "Sid" : "ELBTargetGroupCreate",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateTargetGroup"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:route-id" : "false"
      }
    }
  },
  {
    "Sid" : "APIGatewayModify",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:DELETE",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:UpdateRestApiPolicy"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*",
      "arn:aws:apigateway:*:*/vpclinks",
      "arn:aws:apigateway:*:*/vpclinks/*",
      "arn:aws:apigateway:*:*/tags",
      "arn:aws:apigateway:*:*/tags/*"
    ]
  }
}
```

```
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Sid" : "APIGatewayVpcLinksGet",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*::/vpclinks",
      "arn:aws:apigateway:*::/vpclinks/*"
    ]
  },
  {
    "Sid" : "OrganizationDescribe",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudformationStackCreate",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudformationStackTag",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:TagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/*"
  },
  {
    "Sid" : "CreateRefactorSpacesSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "CreateELBSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
      }
    }
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

説明 : SSM Automation ドキュメントに渡された IAM サービスロールで

AWSRefactorSpacesCreateResources を使用して、オートメーションの実行に必要なアクセス許可を付与します。このポリシーは、自動化の進行状況を追跡するために EC2 タグへの読み取り/書き込みアクセスを許可します。Refactor Spaces 環境のネットワークブリッジが有効になっている場合、環境内の他の Refactor Spaces サービスによるトラフィックを許可するため、オートメーションは環境のセキュリティグループを EC2 インスタンスにも追加します。このポリシーでは、Application Migration Service の起動後アクション SSM パラメータへのアクセスも付与されます。

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpaces-SSMAutomationPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 8 月 10 日 15:08 UTC
- 編集日時: 2023 年 8 月 10 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubRefactorSpacesFullAccess

説明: タグに基づいてスコープダウンできるため、AWS Lambda AWS MigrationHub と AWS Resource Access Manager に必要なアクセス許可を除き、リファクタリングスペース、AWS MigrationHub リファクタリングスペースコンソール機能、およびその他の関連 AWS サービスへのフルアクセスを許可します。

AWSMigrationHubRefactorSpacesFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubRefactorSpacesFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 11 月 29 日 07:12 UTC
- 編集日時: 2024 年 4 月 11 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "ResourceTagTransitGatewayCreate",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTransitGateway",
    "ec2:CreateSecurityGroup",
    "ec2:CreateTransitGatewayVpcAttachment"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
},
{
  "Sid" : "VpcEndpointServiceConfigurationCreate",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpointServiceConfiguration"
  ],
  "Resource" : "*"
},
{
  "Sid" : "EC2NetworkingModify",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteTransitGateway",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTransitGatewayVpcAttachment",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2>DeleteTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/refactor-spaces:environment-id" : "false"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "VpcEndpointServiceConfigurationDelete",
    "Effect" : "Allow",
    "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Sid" : "ELBLoadBalancerCreate",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags",
      "elasticloadbalancing:CreateLoadBalancer"
    ],
    "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/refactor-spaces:application-id" : "false"
      }
    }
  },
  {
    "Sid" : "ELBDescribe",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeTargetHealth",
      "elasticloadbalancing:DescribeTargetGroups",
      "elasticloadbalancing:DescribeListeners"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "ELBModify",
    "Effect" : "Allow",
    "Action" : [
```

```
    "elasticloadbalancing:RegisterTargets",
    "elasticloadbalancing:CreateLoadBalancerListeners",
    "elasticloadbalancing:CreateListener",
    "elasticloadbalancing>DeleteListener",
    "elasticloadbalancing>DeleteTargetGroup"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/refactor-spaces:route-id" : [
        "*"
      ]
    }
  }
},
{
  "Sid" : "ELBLoadBalancerDelete",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteLoadBalancer",
  "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*"
},
{
  "Sid" : "ELBListenerCreate",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:AddTags",
    "elasticloadbalancing:CreateListener"
  ],
  "Resource" : [
    "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
    "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/refactor-spaces:route-id" : "false"
    }
  }
},
{
  "Sid" : "ELBListenerDelete",
  "Effect" : "Allow",
  "Action" : "elasticloadbalancing>DeleteListener",
  "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
```

```
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ],
  {
    "Sid" : "APIGatewayModify",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET",
      "apigateway:DELETE",
      "apigateway:PATCH",
      "apigateway:POST",
      "apigateway:PUT",
      "apigateway:UpdateRestApiPolicy"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*",
      "arn:aws:apigateway:*:*/vpclinks",
      "arn:aws:apigateway:*:*/vpclinks/*",
      "arn:aws:apigateway:*:*/tags",
      "arn:aws:apigateway:*:*/tags*"
    ],
    "Condition" : {
```



```
    "Null" : {
      "aws:ResourceTag/refactor-spaces:application-id" : "false"
    }
  },
  {
    "Sid" : "APIGatewayVpcLinksGet",
    "Effect" : "Allow",
    "Action" : "apigateway:GET",
    "Resource" : [
      "arn:aws:apigateway:*::/vpclinks",
      "arn:aws:apigateway:*::/vpclinks/*"
    ]
  },
  {
    "Sid" : "OrganizationDescribe",
    "Effect" : "Allow",
    "Action" : [
      "organizations:DescribeOrganization"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudformationStackCreate",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:CreateStack"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudformationStackTag",
    "Effect" : "Allow",
    "Action" : [
      "cloudformation:TagResource"
    ],
    "Resource" : "arn:aws:cloudformation:*:*:stack/*"
  },
  {
    "Sid" : "CreateRefactorSpacesSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
```

```
    "StringEquals" : {
      "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
    }
  },
  {
    "Sid" : "CreateELBSLR",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

説明：AWS Migration Hub リファクタリングスペースによって管理または使用される AWS リソースへのアクセスを提供します。

AWSMigrationHubRefactorSpacesServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 29 日 06:50 UTC
- 編集日時: 2023 年 7 月 20 日 15:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubSMSAccess

説明： お客様のアカウントで Migration Hub を呼び出すためのロールを引き受けるための Server Migration Service のポリシー

AWSMigrationHubSMSAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubSMSAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 8 月 14 日 13:57 UTC
- 編集日時: 2019 年 10 月 7 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubStrategyCollector

説明: AWS Migration Hub Strategy Recommendations サービスとの通信、サービスに関連する S3 バケットへの読み取り/書き込みアクセス、ログとメトリクスを にアップロードするための Amazon API Gateway アクセス AWS、認証情報を取得するための AWS Secrets Manager アクセス、および関連する サービスを許可するアクセス許可を付与します。

AWSMigrationHubStrategyCollector は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubStrategyCollector をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 19 日 20:15 UTC
- 編集日時: 2024 年 4 月 1 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Sid" : "MHSRAllowS3Resources",
"Effect" : "Allow",
"Action" : [
  "s3:GetObject",
  "s3:PutObject",
  "s3:GetBucketAcl",
  "s3:CreateBucket",
  "s3:PutEncryptionConfiguration",
  "s3:PutBucketPublicAccessBlock",
  "s3:PutBucketVersioning",
  "s3:PutLifecycleConfiguration",
  "s3:ListBucket",
  "s3:GetBucketLocation"
],
"Resource" : "arn:aws:s3::migrationhub-strategy-*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "MHSRAllowS3ListBucket",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "arn:aws:s3:::*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
  }
}
},
{
  "Sid" : "MHSRAllowMetricsAndLogs",
  "Effect" : "Allow",
  "Action" : [
    "application-transformation:PutMetricData",
    "application-transformation:PutLogData",
    "application-transformation:StartPortingCompatibilityAssessment",
    "application-transformation:GetPortingCompatibilityAssessment",
    "application-transformation:StartPortingRecommendationAssessment",
    "application-transformation:GetPortingRecommendationAssessment"
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "MHSRAllowExecuteAPI",
    "Effect" : "Allow",
    "Action" : [
      "execute-api:Invoke",
      "execute-api:ManageConnections"
    ],
    "Resource" : [
      "arn:aws:execute-api:*:*:*/*/*/*/*/prod/*/*/*/*/put-log-data",
      "arn:aws:execute-api:*:*:*/*/*/*/*/prod/*/*/*/*/put-metric-data"
    ]
  },
  {
    "Sid" : "MHSRAllowCollectorAPI",
    "Effect" : "Allow",
    "Action" : [
      "migrationhub-strategy:RegisterCollector",
      "migrationhub-strategy:GetAntiPattern",
      "migrationhub-strategy:GetMessage",
      "migrationhub-strategy:SendMessage",
      "migrationhub-strategy:ListAntiPatterns",
      "migrationhub-strategy:ListJarArtifacts",
      "migrationhub-strategy:UpdateCollectorConfiguration",
      "migrationhub-strategy:PutLogData",
      "migrationhub-strategy:PutMetricData"
    ],
    "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
  },
  {
    "Sid" : "MHSRAllowSecretsManager",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
}
```

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubStrategyConsoleFullAccess

説明: AWS Migration Hub Strategy Recommendations サービスへのフルアクセスと、 を介した関連 AWS サービスへのアクセスを許可します AWS Management Console。

AWSMigrationHubStrategyConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMigrationHubStrategyConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 10 月 19 日 20:13 UTC
- 編集日時: 2022 年 11 月 9 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMigrationHubStrategyServiceRolePolicy

説明：AWS Migration Hub Strategy Recommendations サービスによって使用または管理される AWS リソースへのアクセスを有効にします。

AWSMigrationHubStrategyServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 19 日 20:02 UTC
- 編集日時: 2021 年 10 月 19 日 20:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMobileHub_FullAccess

説明: このポリシーは、AWS Mobile Hub でプロジェクト (および関連する AWS リソース) を作成、削除、変更するアクセス許可をユーザーに付与するために、任意のユーザー、ロール、またはグループにアタッチできます。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。

AWSMobileHub_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMobileHub_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 5 日 19:56 UTC
- 編集日時: 2019 年 12 月 19 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSMobileHub_ReadOnly

説明：このポリシーは、AWS Mobile Hub でプロジェクトを一覧表示および表示するアクセス許可をユーザーに付与するために、任意のユーザー、ロール、またはグループにアタッチできます。これには、各 Mobile Hub プロジェクトのサンプルモバイルアプリのソースコードを生成およびダウンロードする許可も含まれます。ユーザーは Mobile Hub プロジェクトの設定を変更することはできません。

AWSMobileHub_ReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMobileHub_ReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 5 日 19:55 UTC
- 編集日時: 2018 年 7 月 23 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSMSKReplicatorExecutionRole

説明：MSK クラスター間でデータをレプリケートするアクセス許可を Amazon MSK レプリケーターに付与します。

AWSMSKReplicatorExecutionRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSMSKReplicatorExecutionRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 12 月 6 日 00:07 UTC
- 編集日時: 2024 年 3 月 25 日 21:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [
  "kafka-cluster:Connect",
  "kafka-cluster:DescribeCluster",
  "kafka-cluster:AlterCluster",
  "kafka-cluster:DescribeTopic",
  "kafka-cluster:CreateTopic",
  "kafka-cluster:AlterTopic",
  "kafka-cluster:WriteData",
  "kafka-cluster:ReadData",
  "kafka-cluster:AlterGroup",
  "kafka-cluster:DescribeGroup",
  "kafka-cluster:DescribeTopicDynamicConfiguration",
  "kafka-cluster:AlterTopicDynamicConfiguration",
  "kafka-cluster:WriteDataIdempotently"
],
"Resource" : [
  "arn:aws:kafka:*:*:cluster/*"
]
},
{
  "Sid" : "TopicPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:CreateTopic",
    "kafka-cluster:AlterTopic",
    "kafka-cluster:WriteData",
    "kafka-cluster:ReadData",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:AlterTopicDynamicConfiguration",
    "kafka-cluster:AlterCluster"
  ],
  "Resource" : [
    "arn:aws:kafka:*:*:topic/*/*"
  ]
},
{
  "Sid" : "GroupPermissions",
  "Effect" : "Allow",
  "Action" : [
    "kafka-cluster:AlterGroup",
    "kafka-cluster:DescribeGroup"
  ],
  "Resource" : [
```

```
        "arn:aws:kafka:*:*:group/*/*"  
    ]  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSNetworkFirewallServiceRolePolicy

説明：AWSNetworkFirewall がファイアウォールに必要なリソースを作成および管理できるようにします。

AWSNetworkFirewallServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 17 日 17:17 UTC
- 編集日時: 2023 年 3 月 30 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSNetworkManagerCloudWANServiceRolePolicy

説明 : Core Network に関連付けられたリソース NetworkManager へのアクセスを に許可する

AWSNetworkManagerCloudWANServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 12 日 12:17 UTC
- 編集日時: 2022 年 7 月 12 日 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagagation",
        "ec2:DisableTransitGatewayRouteTablePropagagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSNetworkManagerFullAccess

説明： NetworkManager 経由で Amazon へのフルアクセスを提供します AWS Management Console。

AWSNetworkManagerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 17:37 UTC
- 編集日時: 2019 年 12 月 3 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "networkmanager:*",
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "networkmanager.amazonaws.com"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSNetworkManagerReadOnlyAccess

説明： NetworkManager 経由で Amazon への読み取り専用アクセスを提供します AWS Management Console。

AWSNetworkManagerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSNetworkManagerReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 3 日 17:35 UTC
- 編集日時: 2019 年 12 月 3 日 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSNetworkManagerServiceRolePolicy

説明： グローバルネットワークに関連付けられたリソース NetworkManager へのアクセスを に許可する

AWSNetworkManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 14:03 UTC
- 編集日時: 2022 年 7 月 27 日 19:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorks_FullAccess

説明： へのフルアクセスを提供します AWS OpsWorks。

AWSOpsWorks_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSOpsWorks_FullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 1 月 22 日 16:29 UTC
- 編集日時: 2021 年 1 月 22 日 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksCloudWatchLogs

説明：CWLogs 統合が有効になっている OpsWorks インスタンスがログを出荷し、必要なロググループを作成できるようにします

AWSOpsWorksCloudWatchLogs は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCloudWatchLogs をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 3 月 30 日 17:47 UTC
- 編集日時: 2017 年 3 月 30 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksCMInstanceProfileRole

説明： OpsWorks CM によって起動されたインスタンスの S3 アクセスを提供します。

AWSOpsWorksCMInstanceProfileRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCMInstanceProfileRole をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 24 日 09:48 UTC
- 編集日時: 2021 年 4 月 23 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksCMServiceRole

説明: OpsWorks CM サーバーの作成に使用されるサービスロールポリシー。

AWSOpsWorksCMSERVICERole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksCMSERVICERole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 11 月 24 日 09:49 UTC
- 編集日時: 2021 年 4 月 23 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMSERVICERole

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksInstanceRegistration

説明： AWS OpsWorks スタックに登録する Amazon EC2 インスタンスへのアクセスを提供します。

AWSOpsWorksInstanceRegistration は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksInstanceRegistration をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 6 月 3 日 14:23 UTC
- 編集日時: 2016 年 6 月 3 日 14:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksRegisterCLI_EC2

説明: OpsWorks CLI 経由で EC2 インスタンスを登録できるようにするポリシー

AWSOpsWorksRegisterCLI_EC2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOpsWorksRegisterCLI_EC2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 18 日 15:56 UTC
- 編集日時: 2019 年 6 月 18 日 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOpsWorksRegisterCLI_OnPremises

説明: OpsWorks CLI 経由でオンプレミスインスタンスを登録できるようにするポリシー

AWSOpsWorksRegisterCLI_OnPremises は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSOpsWorksRegisterCLI_OnPremises` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 18 日 15:33 UTC
- 編集日時: 2019 年 6 月 18 日 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOrganizationsFullAccess

説明： AWS Organizations へのフルアクセスを提供します。

AWSOrganizationsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOrganizationsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 6 日 20:31 UTC
- 編集日時: 2024 年 2 月 6 日 17:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSOrganizationsReadOnlyAccess

説明： AWS Organizations への読み取り専用アクセスを提供します。

AWSOrganizationsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOrganizationsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 6 日 20:32 UTC
- 編集日時: 2024 年 6 月 7 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
    }
  ],
}
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "AWSOrganizationsReadOnlyAccount",
    "Effect" : "Allow",
    "Action" : [
      "account:GetAlternateContact",
      "account:GetContactInformation",
      "account:ListRegions",
      "account:GetRegionOptStatus",
      "account:GetPrimaryEmail"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOrganizationsServiceTrustPolicy

説明：顧客設定 AWS のサービスを簡素化するために AWS 承認された他のと信頼を共有することを許可するポリシー。

AWSOrganizationsServiceTrustPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2017 年 10 月 10 日 23:04 UTC
- 編集日時: 2017 年 11 月 1 日 06:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSOutpostsAuthorizeServerPolicy

説明：このポリシーは、オンプレミスネットワークに Outpost サーバーをインストールするためのアクセス許可を付与します。

AWSOutpostsAuthorizeServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSOutpostsAuthorizeServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 1 月 4 日 19:23 UTC
- 編集日時: 2023 年 1 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "outposts:StartConnection",
      "outposts:GetConnection"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSOutpostsServiceRolePolicy

説明： AWS Outposts によって管理される AWS リソースへのアクセスを有効にするサービスリンクロールポリシー

AWSOutpostsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 9 日 22:55 UTC
- 編集日時: 2020 年 11 月 9 日 22:55 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWS Panorama Appliance Role Policy

説明: AWS Panorama アプライアンスの AWS IoT ソフトウェアが Amazon にログをアップロードできるようにします CloudWatch。

AWSPanoramaApplianceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaApplianceServiceRolePolicy

説明 : AWS Panorama アプライアンスが Amazon にログをアップロードし CloudWatch、AWS Panorama で使用するために作成された Amazon S3 アクセスポイントからオブジェクトを取得できるようにします。

AWSPanoramaApplianceServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaApplianceServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:14 UTC
- 編集日時: 2023 年 1 月 17 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaFullAccess

説明： AWS Panorama へのフルアクセスを提供します

AWSPanoramaFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 1 日 13:12 UTC
- 編集日時: 2022 年 1 月 12 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaGreengrassGroupRolePolicy

説明 : AWS Panorama アプライアンスの AWS Lambda 関数が Panorama のリソースを管理し、Amazon にログとメトリクスをアップロードし CloudWatch、Panorama で使用するために作成されたバケット内のオブジェクトを管理できるようにします。

AWSPanoramaGreengrassGroupRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaGreengrassGroupRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:10 UTC
- 編集日時: 2021 年 1 月 6 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaSageMakerRolePolicy

説明： Amazon SageMaker が AWS Panorama で使用するように作成されたバケット内のオブジェクトを管理できるようにします。

AWSPanoramaSageMakerRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaSageMakerRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:13 UTC
- 編集日時: 2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaServiceLinkedRolePolicy

説明： AWS Panorama が AWS IoT、Secrets Manager、および AWS Panorama でリソースを管理できるようにします。AWS

AWSPanoramaServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 10 月 20 日 12:12 UTC
- 編集日時: 2021 年 10 月 20 日 12:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPanoramaServiceRolePolicy

説明 : AWS Panorama が Amazon S3、AWS IoT、AWS IoT GreenGrass、AWS Lambda、Amazon SageMaker、Amazon CloudWatch Logs のリソースを管理し、サービスロールを AWS IoT、IoT、および Amazon に渡すことを許可します SageMaker。AWS IoT GreenGrass AWSPanoramaServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPanoramaServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 12 月 1 日 13:14 UTC
- 編集日時: 2020 年 12 月 1 日 13:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPriceListServiceFullAccess

説明： AWS Price List Service へのフルアクセスを提供します。

AWSPriceListServiceFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPriceListServiceFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 22 日 00:36 UTC
- 編集日時: 2017 年 11 月 22 日 00:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPriateCAAuditor

説明： 監査者に AWS プライベート認証機関へのアクセスを提供する

AWSPriateCAAuditor は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPriateCAAuditor をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:33 UTC
- 編集日時: 2023 年 2 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAAuditor

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPrivateCAFullAccess

説明：AWS プライベート認証機関へのフルアクセスを提供します

AWSPrivateCAFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:20 UTC
- 編集日時: 2023 年 2 月 14 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPrivateCAPrivilegedUser

説明：プライベート認証機関への特権 AWS 証明書ユーザーアクセスを提供する

AWSPrivateCAPrivilegedUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateCAPrivilegedUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:26 UTC
- 編集日時: 2023 年 2 月 14 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPivateCAReadOnly

説明： AWS プライベート認証機関への読み取り専用アクセスを提供する

AWSPivateCAReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPivateCAReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:30 UTC
- 編集日時: 2023 年 2 月 14 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPivateCAReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPriateCAUser

説明：証明書ユーザーに AWS プライベート認証機関へのアクセスを提供します

AWSPriateCAUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPriateCAUser をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 2 月 14 日 18:16 UTC
- 編集日時: 2023 年 2 月 14 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAUser

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPrivateMarketplaceAdminFullAccess

説明： AWS Private Marketplace のすべての管理アクションへのフルアクセスを提供します。

AWSPrivateMarketplaceAdminFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPrivateMarketplaceAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 16:32 UTC
- 編集日時: 2024 年 2 月 14 日 22:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPrivateMarketplaceRequests

説明 : AWS Private Marketplace でリクエストを作成するアクセスを提供します。

AWSPrivateMarketplaceRequests は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSPivateMarketplaceRequests` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 28 日 21:44 UTC
- 編集日時: 2019 年 10 月 28 日 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPivateMarketplaceRequests`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSPrivateNetworksServiceRolePolicy

説明： AWS Private Networks Service がお客様に代わってリソースを管理できるようにします。

AWSPrivateNetworksServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 12 月 16 日 23:17 UTC
- 編集日時: 2021 年 12 月 16 日 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/Private5G"
      }
    }
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSProtonCodeBuildProvisioningBasicAccess

説明：AWS プロトン CodeBuild プロビジョニングのビルドを実行するには、アクセス許可 CodeBuild が必要です。

AWSProtonCodeBuildProvisioningBasicAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonCodeBuildProvisioningBasicAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 9 日 21:04 UTC
- 編集日時: 2022 年 11 月 9 日 21:04 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

説明： AWS Proton がユーザーに代わって CodeBuild およびその他の AWS サービスを使用して Proton リソースプロビジョニングを管理できるようにします。

AWSProtonCodeBuildProvisioningServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 9 日 21:32 UTC
- 編集日時: 2023 年 5 月 17 日 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSProtonDeveloperAccess

説明: AWS Proton APIs とマネジメントコンソールへのアクセスを提供しますが、Proton テンプレートまたは環境の管理は許可しません。

AWSProtonDeveloperAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonDeveloperAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:02 UTC
- 編集日時: 2024 年 6 月 6 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
{
  "Sid" : "ProtonPermissions",
  "Effect" : "Allow",
  "Action" : [
    "codecommit:ListRepositories",
    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineExecution",
    "codepipeline:GetPipelineState",
    "codepipeline:ListPipelineExecutions",
    "codepipeline:ListPipelines",
    "codestar-connections:ListConnections",
    "codestar-connections:UseConnection",
    "proton:CancelServiceInstanceDeployment",
    "proton:CancelServicePipelineDeployment",
    "proton:CreateService",
    "proton>DeleteService",
    "proton:GetAccountRoles",
    "proton:GetAccountSettings",
    "proton:GetEnvironment",
    "proton:GetEnvironmentAccountConnection",
    "proton:GetEnvironmentTemplate",
    "proton:GetEnvironmentTemplateMajorVersion",
    "proton:GetEnvironmentTemplateMinorVersion",
    "proton:GetEnvironmentTemplateVersion",
    "proton:GetRepository",
    "proton:GetRepositorySyncStatus",
    "proton:GetResourcesSummary",
    "proton:GetService",
    "proton:GetServiceInstance",
    "proton:GetServiceTemplate",
    "proton:GetServiceTemplateMajorVersion",
    "proton:GetServiceTemplateMinorVersion",
    "proton:GetServiceTemplateVersion",
    "proton:GetTemplateSyncConfig",
    "proton:GetTemplateSyncStatus",
    "proton:ListEnvironmentAccountConnections",
    "proton:ListEnvironmentOutputs",
    "proton:ListEnvironmentProvisionedResources",
    "proton:ListEnvironments",
    "proton:ListEnvironmentTemplateMajorVersions",
    "proton:ListEnvironmentTemplateMinorVersions",
    "proton:ListEnvironmentTemplates",
    "proton:ListEnvironmentTemplateVersions",
    "proton:ListRepositories",
```



```

    "proton:ListRepositorySyncDefinitions",
    "proton:ListServiceInstanceOutputs",
    "proton:ListServiceInstanceProvisionedResources",
    "proton:ListServiceInstances",
    "proton:ListServicePipelineOutputs",
    "proton:ListServicePipelineProvisionedResources",
    "proton:ListServices",
    "proton:ListServiceTemplateMajorVersions",
    "proton:ListServiceTemplateMinorVersions",
    "proton:ListServiceTemplates",
    "proton:ListServiceTemplateVersions",
    "proton:ListTagsForResource",
    "proton:UpdateService",
    "proton:UpdateServiceInstance",
    "proton:UpdateServicePipeline",
    "s3:ListAllMyBuckets",
    "s3:ListBucket"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CodeStarConnectionsPermissions",
  "Effect" : "Allow",
  "Action" : "codestar-connections:PassConnection",
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
},
{
  "Sid" : "CodeConnectionsPermissions",
  "Effect" : "Allow",
  "Action" : "codeconnections:PassConnection",
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ],
  "Condition" : {
    "StringEquals" : {

```

```
        "codeconnections:PassedToService" : "proton.amazonaws.com"
    }
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSProtonFullAccess

説明： AWS Proton APIs と マネジメントコンソールへのフルアクセスを提供します。これらの許可に加えて、S3 バケットからテンプレートバンドルを登録するには Amazon S3 へのアクセスも必要です。また、Proton のサービスロールを作成および管理するための Amazon IAM へのアクセスも必要です。

AWSProtonFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:07 UTC
- 編集日時: 2024 年 6 月 6 日 18:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Sid" : "CreateServiceLinkedRolePermissions",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : "sync.proton.amazonaws.com"
    }
  }
},
{
  "Sid" : "CodeStarConnectionsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:PassConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections::*:connection/*",
    "arn:aws:codeconnections::*:connection/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "codestar-connections:PassedToService" : "proton.amazonaws.com"
    }
  }
},
{
  "Sid" : "CodeConnectionsPermissions",
  "Effect" : "Allow",
  "Action" : [
    "codeconnections:PassConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections::*:connection/*",
    "arn:aws:codeconnections::*:connection/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "codeconnections:PassedToService" : "proton.amazonaws.com"
    }
  }
}
```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSProtonReadOnlyAccess

説明： AWS Proton APIsとマネジメントコンソールへの読み取り専用アクセスを提供します。

AWSProtonReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSProtonReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 2 月 17 日 19:09 UTC
- 編集日時: 2022 年 11 月 18 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSProtonServiceGitSyncServiceRolePolicy

説明： AWS Proton が git リポジトリから AWS Proton にサービス、環境、コンポーネント定義を同期できるようにするポリシー。

AWSProtonServiceGitSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2023 年 4 月 4 日 15:55 UTC
- 編集日時: 2023 年 4 月 4 日 15:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSProtonSyncServiceRolePolicy

説明： AWS Proton が git リポジトリのコンテンツを Proton に同期したり、 Proton のコンテンツを git リポジトリに同期したりできるようにするポリシー。

AWSProtonSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 23 日 21:14 UTC
- 編集日時: 2024 年 5 月 5 日 01:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton>DeleteServiceTemplateVersion",
        "proton>DeleteEnvironmentTemplateVersion",
        "proton>CreateServiceTemplateVersion",
        "proton>CreateServiceTemplate",
        "proton>CreateEnvironmentTemplateVersion",
        "proton>CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton>CreateEnvironmentTemplateMajorVersion",
        "proton>CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSPurchaseOrdersServiceRolePolicy

説明: 請求コンソールで発注書を表示および変更するアクセス許可を付与します

AWSPurchaseOrdersServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSPurchaseOrdersServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 6 日 18:15 UTC
- 編集日時: 2023 年 7 月 17 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightAssetBundleExportPolicy

説明： QuickSight アセットバンドルエクスポートオペレーションの実行に必要な一連のアクセス許可を提供します。

AWSQuickSightAssetBundleExportPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightAssetBundleExportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 21:31 UTC
- 編集日時: 2024 年 3 月 27 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
```

```
    "quicksight:DescribeDashboardPermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
},
{
  "Sid" : "AnalysisReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeAnalysis",
    "quicksight:DescribeAnalysisPermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:analysis/*"
},
{
  "Sid" : "DataSetReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeDataSet",
    "quicksight:DescribeDataSetRefreshProperties",
    "quicksight:ListRefreshSchedules",
    "quicksight:DescribeDataSetPermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dataset/*"
},
{
  "Sid" : "DataSourceReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeDataSource",
    "quicksight:DescribeDataSourcePermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:datasource/*"
},
{
  "Sid" : "ThemeReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeTheme",
    "quicksight:DescribeThemePermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:theme/*"
},
{
  "Sid" : "VPCConnectionReadAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "quicksight:DescribeVPCConnection",
  "quicksight:ListVPCConnections"
],
"Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
},
{
  "Sid" : "RefreshScheduleReadAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeRefreshSchedule"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
},
{
  "Sid" : "AssetBundleExportOperations",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeAssetBundleExportJob",
    "quicksight:ListAssetBundleExportJobs",
    "quicksight:StartAssetBundleExportJob"
  ],
  "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightAssetBundleImportPolicy

説明：QuickSight アセットバンドルのインポートオペレーションを実行するために必要な一連のアクセス許可を提供します。

AWSQuickSightAssetBundleImportPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightAssetBundleImportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 3 月 27 日 21:40 UTC
- 編集日時: 2024 年 3 月 27 日 21:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*/*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
```



```
"Action" : [
  "quicksight:CreateDashboard",
  "quicksight>DeleteDashboard",
  "quicksight:DescribeDashboard",
  "quicksight:UpdateDashboard",
  "quicksight:UpdateDashboardPublishedVersion",
  "quicksight:DescribeDashboardPermissions",
  "quicksight:UpdateDashboardPermissions",
  "quicksight:UpdateDashboardLinks"
],
"Resource" : "arn:aws:quicksight:*:*:dashboard/*"
},
{
  "Sid" : "AnalysisWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:CreateAnalysis",
    "quicksight>DeleteAnalysis",
    "quicksight:DescribeAnalysis",
    "quicksight:UpdateAnalysis",
    "quicksight:DescribeAnalysisPermissions",
    "quicksight:UpdateAnalysisPermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:analysis/*"
},
{
  "Sid" : "DataSetWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:CreateDataSet",
    "quicksight>DeleteDataSet",
    "quicksight:DescribeDataSet",
    "quicksight:PassDataSet",
    "quicksight:UpdateDataSet",
    "quicksight>DeleteDataSetRefreshProperties",
    "quicksight:DescribeDataSetRefreshProperties",
    "quicksight:PutDataSetRefreshProperties",
    "quicksight:UpdateDataSetPermissions",
    "quicksight:DescribeDataSetPermissions",
    "quicksight:ListRefreshSchedules"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dataset/*"
},
{
```

```
"Sid" : "DataSourceWriteAccess",
"Effect" : "Allow",
"Action" : [
  "quicksight:CreateDataSource",
  "quicksight:DescribeDataSource",
  "quicksight>DeleteDataSource",
  "quicksight:PassDataSource",
  "quicksight:UpdateDataSource",
  "quicksight:UpdateDataSourcePermissions",
  "quicksight:DescribeDataSourcePermissions"
],
"Resource" : "arn:aws:quicksight:*:*:datasource/*"
},
{
  "Sid" : "ThemeWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:CreateTheme",
    "quicksight>DeleteTheme",
    "quicksight:DescribeTheme",
    "quicksight:UpdateTheme",
    "quicksight:DescribeThemePermissions",
    "quicksight:UpdateThemePermissions"
  ],
  "Resource" : "arn:aws:quicksight:*:*:theme/*"
},
{
  "Sid" : "RefreshScheduleWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:CreateRefreshSchedule",
    "quicksight:DescribeRefreshSchedule",
    "quicksight>DeleteRefreshSchedule",
    "quicksight:UpdateRefreshSchedule"
  ],
  "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
},
{
  "Sid" : "VPCConnectionWriteAccess",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:ListVPCConnections",
    "quicksight:CreateVPCConnection",
    "quicksight:DescribeVPCConnection",
```

```
    "quicksight:DeleteVPCConnection",
    "quicksight:UpdateVPCConnection"
  ],
  "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
},
{
  "Sid" : "AssetBundleImportOperations",
  "Effect" : "Allow",
  "Action" : [
    "quicksight:DescribeAssetBundleImportJob",
    "quicksight:ListAssetBundleImportJobs",
    "quicksight:StartAssetBundleImportJob"
  ],
  "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuicksightAthenaAccess

説明： Athena クエリ結果に使用される Athena API および S3 バケットへの Quicksight アクセス

AWSQuicksightAthenaAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuicksightAthenaAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 12 月 9 日 02:31 UTC

- 編集日時: 2021 年 7 月 7 日 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightDescribeRDS

説明： QuickSight が RDS リソースを記述することを許可する

AWSQuickSightDescribeRDS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightDescribeRDS をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2015 年 11 月 10 日 23:24 UTC
- 編集日時: 2015 年 11 月 10 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightDescribeRedshift

説明 : QuickSight が Redshift リソースを記述することを許可する

AWSQuickSightDescribeRedshift は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightDescribeRedshift をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightElasticsearchPolicy

説明： Amazon から Amazon Elasticsearch リソースへのアクセスを提供します QuickSight

AWSQuickSightElasticsearchPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightElasticsearchPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 9 日 17:27 UTC
- 編集日時: 2021 年 9 月 7 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightIoTAnalyticsAccess

説明： IoT Analytics データセットへの QuickSight 読み取り専用アクセスを許可する

AWSQuickSightIoTAnalyticsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightIoTAnalyticsAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 17:00 UTC
- 編集日時: 2017 年 11 月 29 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightListIAM

説明： QuickSight IAM エンティティの一覧表示を許可する

AWSQuickSightListIAM は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightListIAM をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 11 月 10 日 23:25 UTC
- 編集日時: 2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuicksightOpenSearchPolicy

説明 : Amazon から Amazon OpenSearch リソースへのアクセスを提供します QuickSight

AWSQuicksightOpenSearchPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuicksightOpenSearchPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2021 年 9 月 7 日 23:26 UTC
- 編集日時: 2021 年 9 月 7 日 23:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightSageMakerPolicy

説明 : Amazon から Amazon SageMaker リソースへのアクセスを提供します QuickSight

AWSQuickSightSageMakerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightSageMakerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 1 月 17 日 17:18 UTC
- 編集日時: 2023 年 10 月 30 日 17:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
```



```
"Effect" : "Allow",
"Action" : "s3:PutObject",
"Resource" : "arn:aws:s3::sagemaker*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
},
{
  "Sid" : "S3BucketReadAccess",
  "Effect" : "Allow",
  "Action" : "s3:ListBucket",
  "Resource" : "arn:aws:s3::sagemaker*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSQuickSightTimestreamPolicy

説明： AWS Timestream APIs AWS QuickSight へのアクセス。お客様は、このポリシーを AWS QuickSight ロールにアタッチして、データとメタデータの取得を許可できます。

AWSQuickSightTimestreamPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSQuickSightTimestreamPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 9 月 30 日 21:47 UTC

- 編集日時: 2020 年 9 月 30 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSReachabilityAnalyzerServiceRolePolicy

説明： VPC Reachability Analyzer がユーザーに代わって AWS リソースにアクセスし、 AWS Organizations と統合できるようにします。

AWSReachabilityAnalyzerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 23 日 17:12 UTC
- 編集日時: 2024 年 5 月 15 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
"Action" : [  
  "cloudformation:DescribeStacks",  
  "cloudformation:ListStackResources",  
  "directconnect:DescribeConnections",  
  "directconnect:DescribeDirectConnectGatewayAssociations",  
  "directconnect:DescribeDirectConnectGatewayAttachments",  
  "directconnect:DescribeDirectConnectGateways",  
  "directconnect:DescribeVirtualGateways",  
  "directconnect:DescribeVirtualInterfaces",  
  "ec2:DescribeAvailabilityZones",  
  "ec2:DescribeCustomerGateways",  
  "ec2:DescribeInstances",  
  "ec2:DescribeInternetGateways",  
  "ec2:DescribeManagedPrefixLists",  
  "ec2:DescribeNatGateways",  
  "ec2:DescribeNetworkAcls",  
  "ec2:DescribeNetworkInterfaces",  
  "ec2:DescribePrefixLists",  
  "ec2:DescribeRegions",  
  "ec2:DescribeRouteTables",  
  "ec2:DescribeSecurityGroups",  
  "ec2:DescribeSubnets",  
  "ec2:DescribeTransitGatewayAttachments",  
  "ec2:DescribeTransitGatewayConnects",  
  "ec2:DescribeTransitGatewayPeeringAttachments",  
  "ec2:DescribeTransitGatewayRouteTables",  
  "ec2:DescribeTransitGatewayVpcAttachments",  
  "ec2:DescribeTransitGateways",  
  "ec2:DescribeVpcEndpointServiceConfigurations",  
  "ec2:DescribeVpcEndpoints",  
  "ec2:DescribeVpcPeeringConnections",  
  "ec2:DescribeVpcs",  
  "ec2:DescribeVpnConnections",  
  "ec2:DescribeVpnGateways",  
  "ec2:GetManagedPrefixListEntries",  
  "ec2:GetTransitGatewayRouteTablePropagations",  
  "ec2:SearchTransitGatewayRoutes",  
  "elasticloadbalancing:DescribeListeners",  
  "elasticloadbalancing:DescribeLoadBalancerAttributes",  
  "elasticloadbalancing:DescribeLoadBalancers",  
  "elasticloadbalancing:DescribeRules",  
  "elasticloadbalancing:DescribeTags",  
  "elasticloadbalancing:DescribeTargetGroupAttributes",  
  "elasticloadbalancing:DescribeTargetGroups",
```

```
    "elasticloadbalancing:DescribeTargetHealth",
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListCustomRoutingAccelerators",
    "globalaccelerator:ListCustomRoutingEndpointGroups",
    "globalaccelerator:ListCustomRoutingListeners",
    "globalaccelerator:ListCustomRoutingPortMappings",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "resource-groups:ListGroups",
    "resource-groups:ListGroupResources",
    "tag:GetResources",
    "tiros:CreateQuery",
    "tiros:ExtendQuery",
    "tiros:GetQueryAnswer",
    "tiros:GetQueryExplanation",
    "tiros:GetQueryExtensionAccounts"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ApigatewayPermissions",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
```

```
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRefactoringToolkitFullAccess

説明：このポリシーは、Microsoft Visual Studio の AWS Toolkit for .NET リファクタリング拡張機能で AWS サービスを使用するアクセス許可を付与します。ローカル AWS プロファイルにアタッチすることを目的としています。このポリシーにより、アプリケーションアーティファクトのアップロードし、Amazon S3 からの結果のアーティファクトをダウンロードできます。これにより、を使用してアプリケーションをコンテナイメージに構築 AWS CodeBuild し、Amazon Elastic Container Registry (Amazon ECR) からイメージを保存および取得できます。また、Amazon Elastic Container Service (Amazon ECS) AWS などの のコンテナサービスへのアプリケーションのデプロイ、VPC リソースのオプションの作成、AWS ディレクトリサービスなどの既存のインフラストラクチャへのオプション接続、およびその他の関連サービスが可能になります。

AWSRefactoringToolkitFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRefactoringToolkitFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集日時: 2024 年 3 月 25 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn*:cloudformation:*:*:stack/a2c-app-*",
        "arn*:cloudformation:*:*:stack/a2c-build-*",
        "arn*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
    "codebuild:CreateProject",
    "codebuild:UpdateProject"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "CodeBuildExecutionAccess",
  "Effect" : "Allow",
  "Action" : [
    "codebuild:StartBuild"
  ],
  "Resource" : "arn:aws:codebuild:*:*:project/*"
},
{
  "Sid" : "CreateSecurityGroupAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Ec2CreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateInternetGateway",
    "ec2:CreateKeyPair",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:AuthorizeSecurityGroupIngress"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
}
```



```
    }
  },
  {
    "Sid" : "Ec2CreateAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateInternetGateway",
      "ec2:CreateKeyPair",
      "ec2:CreateRoute",
      "ec2:CreateRouteTable",
      "ec2:CreateSubnet",
      "ec2:CreateTags",
      "ec2:CreateVpc",
      "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:RequestTag/application-transformation" : "false"
      }
    }
  },
  {
    "Sid" : "Ec2ModifyAccess",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AssociateRouteTable",
      "ec2:AttachInternetGateway",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2>DeleteTags",
      "ec2:ModifySubnetAttribute",
      "ec2:ModifyVpcAttribute",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateSubnet",
      "ec2:CreateRoute",
      "ec2:CreateRouteTable"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/a2c-generated" : "false"
      }
    }
  },
},
```

```
{
  "Sid" : "Ec2ModifyAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AssociateRouteTable",
    "ec2:AttachInternetGateway",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:DeleteTags",
    "ec2:ModifySubnetAttribute",
    "ec2:ModifyVpcAttribute",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateSubnet",
    "ec2:CreateRoute",
    "ec2:CreateRouteTable"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcrCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr:TagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "EcrCreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecr:CreateRepository",
    "ecr:TagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
```

```
"Condition" : {
  "Null" : {
    "aws:RequestTag/application-transformation" : "false"
  }
},
{
  "Sid" : "EcrModifyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:GetLifecyclePolicy",
    "ecr:GetRepositoryPolicy",
    "ecr:ListImages",
    "ecr:ListTagsForResource",
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
},
{
  "Sid" : "EcrModifyAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecr:GetLifecyclePolicy",
    "ecr:GetRepositoryPolicy",
    "ecr:ListImages",
    "ecr:ListTagsForResource",
    "ecr:TagResource",
    "ecr:UntagResource"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcsCreateAccess",
```

```
"Effect" : "Allow",
"Action" : [
  "ecs:CreateCluster",
  "ecs:CreateService",
  "ecs:RegisterTaskDefinition",
  "ecs:TagResource"
],
"Resource" : "*",
"Condition" : {
  "Null" : {
    "aws:RequestTag/a2c-generated" : "false"
  }
}
},
{
  "Sid" : "EcsCreateAccessATS",
  "Effect" : "Allow",
  "Action" : [
    "ecs:CreateCluster",
    "ecs:CreateService",
    "ecs:RegisterTaskDefinition",
    "ecs:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:RequestTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcsModifyAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecs:UpdateService",
    "ecs:TagResource",
    "ecs:UntagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:ResourceTag/a2c-generated" : "false"
    }
  }
}
```

```
  },
  {
    "Sid" : "EcsModifyAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "ecs:UpdateService",
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/application-transformation" : "false"
      }
    }
  },
  {
    "Sid" : "EcsReadTaskDefinitionAccess",
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeTaskDefinition"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "cloudformation.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "EcsExecuteCommandInSidecar",
    "Effect" : "Allow",
    "Action" : [
      "ecs:ExecuteCommand"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "ecs:container-name" : "a2c-sidecar"
      }
    }
  },
  {
    "Sid" : "EcsExecuteCommandInSidecarATS",
```

```
"Effect" : "Allow",
"Action" : [
  "ecs:ExecuteCommand"
],
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "ecs:container-name" : "application-transformation-sidecar"
  }
}
},
{
  "Sid" : "CreateEcsServiceLinkedRoleAccess",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "ecs.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudwatchCreateAccess",
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:TagResource"
  ],
  "Resource" : [
    "arn:aws:logs::*:log-group:/aws/codebuild/*:*",
    "arn:aws:logs::*:log-group:/aws/ecs/containerinsights/*:*",
    "arn:aws:logs::*:log-group:/aws/ecs/container-logs/*:*"
  ],
  "Condition" : {
    "Null" : {
      "aws:RequestTag/a2c-generated" : "false"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "a2c-generated"
      ]
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "CloudwatchCreateAccessATS",
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:TagResource"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
      "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
    ],
    "Condition" : {
      "Null" : {
        "aws:RequestTag/application-transformation" : "false"
      },
      "ForAllValues:StringEquals" : {
        "aws:TagKeys" : [
          "application-transformation"
        ]
      }
    }
  },
  {
    "Sid" : "CloudwatchGetAccess",
    "Effect" : "Allow",
    "Action" : [
      "logs:GetLogEvents"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
      "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
      "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
    ],
    "Condition" : {
      "Null" : {
        "aws:ResourceTag/a2c-generated" : "false"
      }
    }
  },
  {
    "Sid" : "CloudwatchGetAccessATS",
    "Effect" : "Allow",
```

```
"Action" : [
  "logs:GetLogEvents"
],
"Resource" : [
  "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
  "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
],
"Condition" : {
  "Null" : {
    "aws:ResourceTag/application-transformation" : "false"
  }
}
},
{
  "Sid" : "SsmParameterAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:AddTagsToResource",
    "ssm:GetParameters",
    "ssm:PutParameter",
    "ssm:RemoveTagsFromResource"
  ],
  "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
},
{
  "Sid" : "SsmMessagesAccess",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeSessions",
    "ssmmessages:CreateControlChannel",
    "ssmmessages:CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
  ],
  "Resource" : "*"
},
{
  "Sid" : "S3ObjectAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:PutObject"
  ],
}
```



```
"Resource" : [
  "arn:aws:s3::*/*refactoringtoolkit*",
  "arn:aws:s3::*/*a2c-generated*",
  "arn:aws:s3::*/*application-transformation*"
],
{
  "Sid" : "S3ListAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket"
  ],
  "Resource" : "arn:aws:s3::*:*",
  "Condition" : {
    "StringLike" : {
      "s3:prefix" : [
        "application-transformation",
        "refactoringtoolkit"
      ]
    }
  }
},
{
  "Sid" : "ReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks",
    "clouddirectory:ListDirectories",
    "codebuild:BatchGetProjects",
    "codebuild:BatchGetBuilds",
    "ds:DescribeDirectories",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeRegions",
    "ecr:DescribeImages",
```

```

    "ecr:DescribeRepositories",
    "ecs:DescribeClusters",
    "ecs:DescribeServices",
    "ecs:DescribeTasks",
    "ecs:ListTagsForResource",
    "ecs:ListTasks",
    "iam:ListRoles",
    "s3:GetBucketLocation",
    "s3:GetBucketVersioning",
    "s3:ListAllMyBuckets",
    "secretsmanager:ListSecrets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "GetECSSLR",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
},
{
  "Sid" : "PortingAssistantFullAccess",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
    "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
  ]
},
{
  "Sid" : "ApplicationTransformationAccess",
  "Effect" : "Allow",
  "Action" : [
    "application-transformation:StartPortingCompatibilityAssessment",
    "application-transformation:GetPortingCompatibilityAssessment",
    "application-transformation:StartPortingRecommendationAssessment",
    "application-transformation:GetPortingRecommendationAssessment",
    "application-transformation:PutLogData",
    "application-transformation:PutMetricData",
    "application-transformation:StartContainerization",
    "application-transformation:GetContainerization",

```

```
    "application-transformation:StartDeployment",
    "application-transformation:GetDeployment"
  ],
  "Resource" : "*"
},
{
  "Sid" : "KmsAccess",
  "Effect" : "Allow",
  "Action" : [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource" : "arn:aws:kms:*:*:*",
  "Condition" : {
    "ForAnyValue:StringLike" : {
      "kms:ResourceAliases" : "alias/application-transformation*"
    }
  }
},
{
  "Sid" : "EcrPushAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:InitiateLayerUpload",
    "ecr:PutImage",
    "ecr:UploadLayerPart",
    "ecr:CompleteLayerUpload",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource" : "arn:*:ecr:*:*:repository/*",
  "Condition" : {
    "Null" : {
      "ecr:ResourceTag/application-transformation" : "false"
    }
  }
},
{
  "Sid" : "EcrAuthAccess",
  "Effect" : "Allow",
  "Action" : [
    "ecr:GetAuthorizationToken"
  ]
}
```

```
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "KmsCreateGrantAccess",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "arn:aws:kms:*:*:*",
    "Condition" : {
      "Bool" : {
        "kms:GrantIsForAWSResource" : true
      },
      "ForAnyValue:StringLike" : {
        "kms:ResourceAliases" : "alias/application-transformation*"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSRefactoringToolkitSidecarPolicy

説明: このポリシーは、Microsoft Visual Studio の AWS Toolkit for .NET リファクタリング拡張機能 AWS を使用してアプリケーションをテストするために作成された Amazon ECS タスクによって使用されることを目的としています。このポリシーは、Amazon S3 からのアプリケーションアーティファクトのダウンロード、Systems Manager を使用したタスクのステータスの伝達、およびその他の必要なサービスへのアクセスを許可します。 AWS

AWSRefactoringToolkitSidecarPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSRefactoringToolkitSidecarPolicy` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 10 月 25 日 16:41 UTC
- 編集日時: 2022 年 10 月 29 日 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSrePostPrivateCloudWatchAccess

説明 : re:Post プライベートアクセスを提供して CloudWatch メトリクスデータを公開する

AWSrePostPrivateCloudWatchAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 15 日 16:37 UTC
- 編集日時: 2023 年 11 月 15 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRepostSpaceSupportOperationsPolicy

説明：このポリシーにより、re:Post Space サービスは、Space アプリケーションを通じて作成されるサポートケースを作成、管理、解決できます。

AWSRepostSpaceSupportOperationsPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRepostSpaceSupportOperationsPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 26 日 21:52 UTC
- 編集日時: 2023 年 11 月 26 日 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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



```
"Sid" : "RepostSpaceSupportOperations",
"Effect" : "Allow",
"Action" : [
  "support:AddAttachmentsToSet",
  "support:AddCommunicationToCase",
  "support:CreateCase",
  "support:DescribeCases",
  "support:DescribeCommunications",
  "support:ResolveCase"
],
"Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResilienceHubAssessmentExecutionPolicy

説明： 評価を実行するために他の サービスへのアクセスを許可する AWS Resilience Hub AWS サービスロールのポリシー。

AWSResilienceHubAssessmentExecutionPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResilienceHubAssessmentExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 6 月 27 日 12:32 UTC
- 編集日時: 2024 年 3 月 24 日 18:05 UTC

- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
```

```
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeLimits",
"dynamodb:DescribeTable",
"dynamodb:ListGlobalTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeFastSnapshotRestores",
"ec2:DescribeFleets",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeNatGateways",
"ec2:DescribePlacementGroups",
"ec2:DescribeRegions",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ecr:DescribeRegistry",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:DescribeServices",
"ecs:DescribeTaskDefinition",
"ecs:ListContainerInstances",
"ecs:ListServices",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeSnapshots",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"fis:GetExperimentTemplate",
```

```
"fis:ListExperimentTemplates",
"fis:ListExperiments",
"fsx:DescribeFileSystems",
"lambda:GetFunctionConcurrency",
"lambda:GetFunctionConfiguration",
"lambda:ListAliases",
"lambda:ListVersionsByFunction",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyTargets",
"rds:DescribeDBSnapshots",
"rds:DescribeGlobalClusters",
"resource-groups:GetGroup",
"resource-groups:ListGroupResources",
"route53-recovery-control-config:ListClusters",
"route53-recovery-control-config:ListControlPanels",
"route53-recovery-control-config:ListRoutingControls",
"route53-recovery-readiness:GetReadinessCheckStatus",
"route53-recovery-readiness:GetResourceSet",
"route53-recovery-readiness:ListReadinessChecks",
"route53:GetHealthCheck",
"route53:ListHealthChecks",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"route53resolver:ListResolverEndpoints",
"route53resolver:ListResolverEndpointIpAddresses",
"s3:GetBucketLocation",
"s3:GetBucketLogging",
"s3:GetBucketObjectLockConfiguration",
"s3:GetBucketPolicyStatus",
"s3:GetBucketTagging",
"s3:GetBucketVersioning",
"s3:GetMultiRegionAccessPointRoutes",
"s3:GetReplicationConfiguration",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"servicecatalog:GetApplication",
"servicecatalog:ListAssociatedResources",
"sns:GetSubscriptionAttributes",
"sns:GetTopicAttributes",
```

```
    "sns:ListSubscriptionsByTopic",
    "sqs:GetQueueAttributes",
    "sqs:GetQueueUrl",
    "ssm:DescribeAutomationExecutions",
    "states:DescribeStateMachine",
    "states:ListStateMachineVersions",
    "states:ListStateMachineAliases",
    "tag:GetResources"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSResilienceHubApiGatewayStatement",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis/*",
    "arn:aws:apigateway:*::/restapis/*",
    "arn:aws:apigateway:*::/usageplans"
  ]
},
{
  "Sid" : "AWSResilienceHubS3Statement",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
},
{
  "Sid" : "AWSResilienceHubCloudWatchStatement",
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:PutMetricData"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "cloudwatch:namespace" : "ResilienceHub"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "AWSResilienceHubSSMStatement",
    "Effect" : "Allow",
    "Action" : [
      "ssm:GetParametersByPath"
    ],
    "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceAccessManagerFullAccess

説明 : AWS Resource Access Manager へのフルアクセスを提供します

AWSResourceAccessManagerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceAccessManagerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 4 日 17:28 UTC
- 編集日時: 2019 年 6 月 4 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceAccessManagerReadOnlyAccess

説明 : AWS Resource Access Manager への読み取り専用アクセスを提供します。

AWSResourceAccessManagerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSResourceAccessManagerReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 9 日 20:58 UTC
- 編集日時: 2019 年 12 月 9 日 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSResourceAccessManagerResourceShareParticipantAccess

説明：AWS リソース共有参加者が必要とする Resource Access Manager APIs へのアクセスを提供します。

AWSResourceAccessManagerResourceShareParticipantAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

AWSResourceAccessManagerResourceShareParticipantAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 9 日 20:41 UTC
- 編集日時: 2019 年 12 月 9 日 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceAccessManagerServiceRolePolicy

説明：顧客の Organizations 構造への読み取り専用 AWS Resource Access Manager アクセスを含むポリシー。ロールを自己削除するための IAM アクセス許可も含まれます。

AWSResourceAccessManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2018 年 11 月 14 日 19:28 UTC
- 編集日時: 2018 年 11 月 14 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

```
    ]
  }
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSResourceExplorerFullAccess

説明: このポリシーは、Resource Explorer リソースにアクセスするための管理アクセス許可を付与し、このアクセスをサポートするために他の AWS のサービスに読み取り専用アクセス許可を付与します。

AWSResourceExplorerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 7 日 20:01 UTC
- 編集日時: 2023 年 11 月 14 日 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceExplorerOrganizationsAccess

説明: このポリシーは、Resource Explorer に管理アクセス許可を付与し、このアクセスをサポートするために他の AWS のサービスに読み取り専用アクセス許可を付与します。AWS Organizations 管理者は、コンソールでマルチアカウント検索を設定および管理するために、これらのアクセス許可が必要です。

AWSResourceExplorerOrganizationsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 14 日 17:01 UTC
- 編集日時: 2023 年 11 月 14 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceExplorerReadOnlyAccess

説明：このポリシーは、Resource Explorer リソースを検索して表示するための読み取り専用アクセス許可を付与し、このアクセスをサポートするために他の AWS のサービスに読み取り専用アクセス許可を付与します。

AWSResourceExplorerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceExplorerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 7 日 19:56 UTC
- 編集日時: 2023 年 11 月 14 日 16:43 UTC

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

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

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

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceExplorerServiceRolePolicy

説明： Resource Explorer がユーザーに代わってリソースと CloudTrail イベントを表示して、検索するリソースのインデックスを作成できます。

AWSResourceExplorerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 10 月 25 日 20:35 UTC
- 編集日時: 2023 年 12 月 20 日 13:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
    ]
  },
  {
    "Sid" : "ApiGatewayAccess",
    "Effect" : "Allow",
    "Action" : [
      "apigateway:GET"
    ],
    "Resource" : [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*/deployments"
    ]
  },
  {
    "Sid" : "ResourceInventoryAccess",
    "Effect" : "Allow",
    "Action" : [
      "access-analyzer:ListAnalyzers",
      "acm-pca:ListCertificateAuthorities",
      "amplify:ListApps",
      "amplify:ListBackendEnvironments",
      "amplify:ListBranches",
      "amplify:ListDomainAssociations",
      "amplifyuibuilder:ListComponents",
      "amplifyuibuilder:ListThemes",
      "app-integrations:ListEventIntegrations",
      "apprunner:ListServices",
      "apprunner:ListVpcConnectors",
      "appstream:DescribeAppBlocks",
      "appstream:DescribeApplications",
      "appstream:DescribeFleets",
      "appstream:DescribeImageBuilders",
      "appstream:DescribeStacks",
      "appsync:ListGraphQLApis",
      "aps:ListRuleGroupsNamespaces",
      "aps:ListWorkspaces",
      "athena:ListDataCatalogs",
      "athena:ListWorkGroups",
      "autoscaling:DescribeAutoScalingGroups",
      "backup:ListBackupPlans",
      "backup:ListReportPlans",
```

```
"batch:DescribeComputeEnvironments",
"batch:DescribeJobQueues",
"batch:ListSchedulingPolicies",
"cloudformation:ListStacks",
"cloudformation:ListStackSets",
"cloudfront:ListCachePolicies",
"cloudfront:ListCloudFrontOriginAccessIdentities",
"cloudfront:ListDistributions",
"cloudfront:ListFieldLevelEncryptionConfigs",
"cloudfront:ListFieldLevelEncryptionProfiles",
"cloudfront:ListFunctions",
"cloudfront:ListOriginAccessControls",
"cloudfront:ListOriginRequestPolicies",
"cloudfront:ListRealtimeLogConfigs",
"cloudfront:ListResponseHeadersPolicies",
"cloudtrail:ListTrails",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:ListDashboards",
"cloudwatch:ListMetricStreams",
"codeartifact:ListDomains",
"codeartifact:ListRepositories",
"codebuild:ListProjects",
"codecommit:ListRepositories",
"codeguru-profiler:ListProfilingGroups",
"codepipeline:ListPipelines",
"codestar-connections:ListConnections",
"cognito-identity:ListIdentityPools",
"cognito-idp:ListUserPools",
"databrew:ListDatasets",
"databrew:ListRecipes",
"databrew:ListRulesets",
"detective:ListGraphs",
"ds:DescribeDirectories",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"ec2:DescribeAddresses",
"ec2:DescribeCapacityReservationFleets",
"ec2:DescribeCapacityReservations",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
```

```
"ec2:DescribeElasticGpus",
"ec2:DescribeExportImageTasks",
"ec2:DescribeExportTasks",
"ec2:DescribeFleets",
"ec2:DescribeFlowLogs",
"ec2:DescribeFpgaImages",
"ec2:DescribeHostReservations",
"ec2:DescribeHosts",
"ec2:DescribeImages",
"ec2:DescribeImportImageTasks",
"ec2:DescribeImportSnapshotTasks",
"ec2:DescribeInstanceEventWindows",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeIpamPools",
"ec2:DescribeIpams",
"ec2:DescribeIpamScopes",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInsightsAccessScopeAnalyses",
"ec2:DescribeNetworkInsightsAccessScopes",
"ec2:DescribeNetworkInsightsAnalyses",
"ec2:DescribeNetworkInsightsPaths",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribePlacementGroups",
"ec2:DescribePublicIpv4Pools",
"ec2:DescribeReservedInstances",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotInstanceRequests",
"ec2:DescribeSubnets",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayConnectPeers",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPolicyTables",
```

```
"ec2:DescribeTransitGatewayRouteTableAnnouncements",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeVerifiedAccessEndpoints",
"ec2:DescribeVerifiedAccessGroups",
"ec2:DescribeVerifiedAccessInstances",
"ec2:DescribeVerifiedAccessTrustProviders",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:GetSubnetCidrReservations",
"ecr:DescribeRepositories",
"ecr-public:DescribeRepositories",
"ecs:DescribeCapacityProviders",
"ecs:DescribeServices",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:ListServices",
"ecs:ListTaskDefinitions",
"ecs:ListTasks",
"elasticache:DescribeCacheClusters",
"elasticache:DescribeCacheParameterGroups",
"elasticache:DescribeCacheSecurityGroups",
"elasticache:DescribeCacheSubnetGroups",
"elasticache:DescribeGlobalReplicationGroups",
"elasticache:DescribeReplicationGroups",
"elasticache:DescribeReservedCacheNodes",
"elasticache:DescribeSnapshots",
"elasticache:DescribeUserGroups",
"elasticache:DescribeUsers",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeEnvironments",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeRules",
"elasticloadbalancing:DescribeTargetGroups",
"emr-serverless:ListApplications",
```

```
"es:ListDomainNames",
"events:ListEventBuses",
"events:ListRules",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"finspace:ListEnvironments",
"firehose:ListDeliveryStreams",
"fis:ListExperimentTemplates",
"forecast:ListDatasetGroups",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"frauddetector:GetEntityTypeTypes",
"frauddetector:GetEventTypes",
"frauddetector:GetLabels",
"frauddetector:GetOutcomes",
"frauddetector:GetVariables",
"gamelift:ListAliases",
"geo:ListPlaceIndexes",
"geo:ListTrackers",
"greengrass:ListComponents",
"globalaccelerator:ListAccelerators",
"globalaccelerator:ListEndpointGroups",
"globalaccelerator:ListListeners",
"glue:GetDatabases",
"glue:GetJobs",
"glue:GetTables",
"glue:GetTriggers",
"greengrass:ListComponentVersions",
"greengrass:ListGroups",
"healthlake:ListFHIRDatastores",
"iam:ListGroups",
"iam:ListInstanceProfiles",
"iam:ListOpenIDConnectProviders",
"iam:ListPolicies",
"iam:ListRoles",
"iam:ListSAMLProviders",
"iam:ListServerCertificates",
"iam:ListUsers",
"iam:ListVirtualMFADevices",
"imagebuilder:ListComponentBuildVersions",
"imagebuilder:ListComponents",
"imagebuilder:ListContainerRecipes",
```

```
"imagebuilder:ListDistributionConfigurations",
"imagebuilder:ListImageBuildVersions",
"imagebuilder:ListImagePipelines",
"imagebuilder:ListImageRecipes",
"imagebuilder:ListImages",
"imagebuilder:ListInfrastructureConfigurations",
"iotanalytics:ListChannels",
"iotanalytics:ListDatasets",
"iotanalytics:ListDatastores",
"iotanalytics:ListPipelines",
"iotevents:ListAlarmModels",
"iotevents:ListDetectorModels",
"iotevents:ListInputs",
"iot:ListJobTemplates",
"iot:ListAuthorizers",
"iot:ListMitigationActions",
"iot:ListPolicies",
"iot:ListProvisioningTemplates",
"iot:ListRoleAliases",
"iot:ListSecurityProfiles",
"iot:ListThings",
"iot:ListTopicRuleDestinations",
"iot:ListTopicRules",
"iotsitewise:ListAssetModels",
"iotsitewise:ListAssets",
"iotsitewise:ListGateways",
"iottwinmaker:ListComponentTypes",
"iottwinmaker:ListEntities",
"iottwinmaker:ListScenes",
"iottwinmaker:ListWorkspaces",
"kafka:ListConfigurations",
"kms:ListKeys",
"ivs:ListChannels",
"ivs:ListStreamKeys",
"kafka:ListClusters",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisvideo:ListStreams",
"lambda:ListAliases",
"lambda:ListCodeSigningConfigs",
"lambda:ListEventSourceMappings",
"lambda:ListFunctions",
"lambda:ListLayers",
```



```
"lambda:ListLayerVersions",
"lex:ListBots",
"lex:ListBotAliases",
"logs:DescribeDestinations",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"lookoutmetrics:ListAlerts",
"lookoutvision:ListProjects",
"mediapackage:ListChannels",
"mediapackage:ListOriginEndpoints",
"mediapackage-vod:ListPackagingConfigurations",
"mediapackage-vod:ListPackagingGroups",
"mq:ListBrokers",
"mediatailor:ListPlaybackConfigurations",
"memorydb:DescribeACLs",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeUsers",
"mobiletargeting:GetApps",
"mobiletargeting:GetSegments",
"mobiletargeting:ListTemplates",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetDevices",
"networkmanager:GetLinks",
"networkmanager:ListAttachments",
"networkmanager:ListCoreNetworks",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:ListAccounts",
"organizations:ListAWSServiceAccessForOrganization",
"organizations:ListDelegatedAdministrators",
"panorama:ListPackages",
"personalize:ListDatasetGroups",
"personalize:ListDatasets",
"personalize:ListSchemas",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListLedgers",
"rds:DescribeBlueGreenDeployments",
"rds:DescribeDBClusterEndpoints",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
```

```
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstanceAutomatedBackups",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBProxies",
"rds:DescribeDBProxyEndpoints",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:DescribeGlobalClusters",
"rds:DescribeOptionGroups",
"rds:DescribeReservedDBInstances",
"redshift:DescribeClusterParameterGroups",
"redshift:DescribeClusters",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"redshift:DescribeEventSubscriptions",
"redshift:DescribeSnapshotCopyGrants",
"redshift:DescribeSnapshotSchedules",
"redshift:DescribeUsageLimits",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"rekognition:DescribeProjects",
"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:ListModel",
"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" : [
  "*"
]
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSResourceGroupsReadOnlyAccess

説明：これは AWS Resource Groups の読み取り専用ポリシーです

AWSResourceGroupsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSResourceGroupsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 10:27 UTC
- 編集日時: 2019 年 2 月 5 日 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRoboMaker_FullAccess

説明： AWS Management Console および SDK AWS RoboMaker 経由で へのフルアクセスを提供します。関連サービス (S3 や IAM など) への限定アクセスも提供します。

AWSRoboMaker_FullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMaker_FullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 10 日 18:34 UTC
- 編集日時: 2021 年 9 月 16 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

ポリシーのバージョニング

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]
```

```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRoboMakerReadOnlyAccess

説明： AWS Management Console および SDK AWS RoboMaker 経由で への読み取り専用アクセスを提供します

AWSRoboMakerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMakerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 26 日 05:30 UTC
- 編集日時: 2020 年 8 月 28 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRoboMakerServicePolicy

説明： RoboMaker サービスポリシー

AWSRoboMakerServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 06:30 UTC
- 編集日時: 2021 年 11 月 11 日 22:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSRoboMakerServiceRolePolicy

説明： RoboMaker サービスポリシー

AWSRoboMakerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSRoboMakerServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 26 日 05:33 UTC
- 編集日時: 2018 年 11 月 26 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSRolesAnywhereServicePolicy

説明 : IAM Roles Anywhere がサービス/使用状況メトリクスを に発行 CloudWatch し、ユーザーに代わってプライベート認証機関のステータスを確認できるようにします。

AWSRolesAnywhereServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 7 月 5 日 15:26 UTC
- 編集日時: 2022 年 7 月 5 日 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSS3OnOutpostsServiceRolePolicy

説明： Amazon S3 on Outposts サービスがユーザーに代わって EC2 ネットワークリソースを管理できるようにします。

AWSS30nOutpostsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 10 月 3 日 20:32 UTC
- 編集日時: 2023 年 10 月 3 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSS30nOutpostsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSavingsPlansFullAccess

説明 : Savings Plans サービスへのフルアクセスを提供します

AWSSavingsPlansFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSavingsPlansFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSavingsPlansReadOnlyAccess

説明： Savings Plans サービスへの読み取り専用アクセスを提供します

AWSSavingsPlansReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSavingsPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 6 日 22:45 UTC
- 編集日時: 2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSecurityHubFullAccess

説明： AWS Security Hub を使用するためのフルアクセスを提供します。

AWSSecurityHubFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityHubFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 23:54 UTC
- 編集日時: 2024 年 4 月 23 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
```

```
"Action" : [
  "guardduty:GetDetector",
  "guardduty:ListDetectors",
  "inspector2:BatchGetAccountStatus",
  "pricing:GetProducts"
],
"Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSecurityHubOrganizationsAccess

説明: 組織内の AWS Security Hub を有効化および管理するためのアクセス許可を付与します。組織全体でサービスの有効化およびサービスの委任管理者アカウントの決定が含まれます。

AWSecurityHubOrganizationsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSecurityHubOrganizationsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2021 年 3 月 15 日 20:53 UTC
- 編集日時: 2023 年 11 月 16 日 21:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSecurityHubReadOnlyAccess

説明： AWS Security Hub リソースへの読み取り専用アクセスを提供します

AWSSecurityHubReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSecurityHubReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 28 日 01:34 UTC
- 編集日時: 2024 年 2 月 22 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSecurityHubServiceRolePolicy

説明 : AWS Security Hub がリソースにアクセスするために必要なサービスにリンクされたロール。

AWSSecurityHubServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 27 日 23:47 UTC
- 編集日時: 2023 年 11 月 27 日 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v14 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogAdminFullAccess

説明： サービスカタログ管理機能へのフルアクセスを提供します

AWSServiceCatalogAdminFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAdminFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 15 日 17:19 UTC
- 編集日時: 2023 年 4 月 13 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
}
```



```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogAdminReadOnlyAccess

説明： Service Catalog 管理者機能への読み取り専用アクセスを提供します

AWSServiceCatalogAdminReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAdminReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 25 日 18:53 UTC
- 編集日時: 2019 年 10 月 25 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogAppRegistryFullAccess

説明： Service Catalog App Registry 機能へのフルアクセスを提供します

AWSServiceCatalogAppRegistryFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAppRegistryFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 12 日 22:25 UTC
- 編集日時: 2023 年 12 月 7 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*:*:*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

説明： Service Catalog アプリケーションレジストリ機能への読み取り専用アクセスを提供します

AWSServiceCatalogAppRegistryReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogAppRegistryReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 12 日 22:34 UTC
- 編集日時: 2022 年 11 月 17 日 18:16 UTC

- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicelog:GetApplication",
        "servicelog>ListApplications",
        "servicelog:GetAssociatedResource",
        "servicelog>ListAssociatedResources",
        "servicelog>ListAssociatedAttributeGroups",
        "servicelog:GetAttributeGroup",
        "servicelog>ListAttributeGroups",
        "servicelog>ListTagsForResource",
        "servicelog>ListAttributeGroupsForApplication",
        "servicelog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

説明 : Service Catalog AppRegistry がユーザーに代わって Resource Groups を管理できるようにします

AWSServiceCatalogAppRegistryServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 5 月 18 日 22:18 UTC
- 編集日時: 2022 年 10 月 26 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
  ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogEndUserFullAccess

説明： サービスカタログのエンドユーザー機能へのフルアクセスを提供します

AWSServiceCatalogEndUserFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogEndUserFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 2 月 15 日 17:22 UTC
- 編集日時: 2019 年 7 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogEndUserReadOnlyAccess

説明： Service Catalog エンドユーザー機能への読み取り専用アクセスを提供します

AWSServiceCatalogEndUserReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSServiceCatalogEndUserReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 10 月 25 日 18:49 UTC
- 編集日時: 2019 年 10 月 25 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

説明： AWS Organizations 組織構造と同期 AWS ServiceCatalog するための のサービスリンクロールポリシー

AWSServiceCatalogOrgsDataSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 10 日 20:48 UTC
- 編集日時: 2023 年 4 月 10 日 20:48 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceCatalogSyncServiceRolePolicy

説明： ソースリポジトリからプロビジョニングアーティファクトを同期 AWS ServiceCatalog するための のサービスリンクロール

AWSServiceCatalogSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 15 日 21:20 UTC
- 編集日時: 2024 年 5 月 3 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
```

```
"Action" : [
  "servicecatalog:ListProvisioningArtifacts",
  "servicecatalog:DescribeProductAsAdmin",
  "servicecatalog>DeleteProvisioningArtifact",
  "servicecatalog:ListServiceActionsForProvisioningArtifact",
  "servicecatalog:DescribeProvisioningArtifact",
  "servicecatalog>CreateProvisioningArtifact",
  "servicecatalog:UpdateProvisioningArtifact"
],
"Resource" : "*"
},
{
  "Sid" : "AccessArtifactRepositories",
  "Effect" : "Allow",
  "Action" : [
    "codestar-connections:UseConnection",
    "codeconnections:UseConnection"
  ],
  "Resource" : [
    "arn:aws:codestar-connections:*:*:connection/*",
    "arn:aws:codeconnections:*:*:connection/*"
  ]
},
{
  "Sid" : "ValidateTemplate",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:ValidateTemplate"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForAmazonEKSNodegroup

説明：顧客のアカウントでノードグループを管理するために必要なアクセス許可。これらのポリシーは、AutoscalingGroups SecurityGroups、LaunchTemplates および リソースの管理に関連しています InstanceProfiles。

AWSServiceRoleForAmazonEKSNodegroup は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 7 日 01:34 UTC
- 編集日時: 2024 年 1 月 4 日 20:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForAmazonQDeveloper

説明：このサービスにリンクされたロールは、Amazon Q デベロッパーが使用状況情報を提供できるようにします。

AWSServiceRoleForAmazonQDeveloper は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 25 日 07:40 UTC
- 編集日時: 2024 年 4 月 25 日 07:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
```



```
"Action" : [
  "cloudwatch:PutMetricData"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "cloudwatch:namespace" : [
      "AWS/Q"
    ]
  }
}
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY

説明： CloudWatch アラームで使用される Systems Manager リソースへのアクセスを提供します

AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 10 月 1 日 09:49 UTC
- 編集日時: 2020 年 10 月 1 日 09:49 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMSERVICE_ROLE_POLICY`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

説明: CloudWatch がユーザーに代わって RDS Performance Insights メトリクスにアクセスすることを許可する

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 9 月 7 日 09:32 UTC
- 編集日時: 2023 年 9 月 7 日 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

```
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForCodeGuru-Profiler

説明： Amazon CodeGuru Profiler がユーザーに代わって通知を送信するために必要なサービスにリンクされたロール。

AWSServiceRoleForCodeGuru-Profiler は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 26 日 22:04 UTC
- 編集日時: 2020 年 6 月 26 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForCodeWhispererPolicy

説明: このロールは CodeWhisperer、アカウント内のデータにアクセスして請求を計算するアクセス許可を に付与し、Amazon でセキュリティレポートを作成およびアクセスし CodeGuru、 にデータを発行するアクセス許可を付与します CloudWatch。

AWSServiceRoleForCodeWhispererPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 24 日 19:39 UTC

- 編集日時：2024 年 3 月 29 日 22:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
    },
  ],
}
```

```
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "sid3",
    "Effect" : "Allow",
    "Action" : [
      "codeguru-security:CreateUploadUrl"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "sid4",
    "Effect" : "Allow",
    "Action" : [
      "codeguru-security:CreateScan",
      "codeguru-security:GetScan",
      "codeguru-security:ListFindings",
      "codeguru-security:GetFindings"
    ],
    "Resource" : [
      "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
    ]
  },
  {
    "Sid" : "sid5",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/CodeWhisperer"
        ]
      }
    }
  }
]
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForEC2ScheduledInstances

説明： EC2 スケジュールされたインスタンスがスポットインスタンスを起動および管理できるようにします。

AWSServiceRoleForEC2ScheduledInstances は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 10 月 12 日 18:31 UTC
- 編集日時: 2017 年 10 月 12 日 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

説明：このサービスにリンクされたロール AWS GroundStation を使用して EC2 を呼び出し、パブリック IPv4 アドレスを検索します

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 12 月 13 日 23:52 UTC
- 編集日時: 2022 年 12 月 13 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForImageBuilder

説明： EC2ImageBuilder がユーザーに代わって AWS サービスを呼び出すことを許可します。

AWSServiceRoleForImageBuilder は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 29 日 22:02 UTC
- 編集日時: 2023 年 10 月 19 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

ポリシーのバージョン

ポリシーのバージョン: v19 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    ]
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForIoTSiteWise

説明: ゲートウェイのプロビジョニングと管理、およびデータのクエリを AWS IoT SiteWise に許可します。このポリシーには、グループにデプロイするために必要な AWS Greengrass アクセス許可、サービスプレフィックス付き関数を作成および更新するための AWS Lambda アクセス許可、およびデータストアからデータをクエリするための AWS IoT Analytics アクセス許可が含まれます。

AWSServiceRoleForIoTSiteWise は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 14 日 19:19 UTC
- 編集日時: 2023 年 11 月 13 日 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITewise"
          ]
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForLogDeliveryPolicy

説明： ログ配信サービスがユーザーに代わってログの送信先を呼び出してログを配信できるようにします。

AWSServiceRoleForLogDeliveryPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 4 日 17:31 UTC
- 編集日時: 2021 年 7 月 15 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
```



```
    "firehose:PutRecordBatch",
    "firehose:ListTagsForDeliveryStream"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/LogDeliveryEnabled" : "true"
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForMonitronPolicy

説明：ユーザーに代わって AWS SSO ユーザー割り当てを含む AWS リソースを管理するためのアクセス許可を Amazon Monitron に付与します。

AWSServiceRoleForMonitronPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 2 日 19:06 UTC
- 編集日時: 2022 年 9 月 29 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForNeptuneGraphPolicy

説明： Amazon Neptune の運用および使用状況のメトリクスとログを公開するための Cloudwatch アクセスを提供します

AWSServiceRoleForNeptuneGraphPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 29 日 14:03 UTC
- 編集日時: 2023 年 11 月 29 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
      }
    }
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

説明 : Private Marketplace リソースを記述および更新し、AWS Organizations を記述するアクセス許可を付与します

AWSServiceRoleForPrivateMarketplaceAdminPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 2 月 14 日 22:28 UTC
- 編集日時: 2024 年 2 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForSMS

説明： EC2、AWS、S3、Cloudformation、AWS を含む へのサービスインスタンスの移行に必要なサービスとリソースへのアクセスを提供します。 EC2, S3

AWSServiceRoleForSMS は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 18:39 UTC

- 編集日時: 2020 年 10 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

ポリシーのバージョン

ポリシーのバージョン: v10 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRoleForUserSubscriptions

説明：サブスクリプションを自動的に更新するために、Identity Center リソースへのユーザーサブスクリプションサービスへのアクセスを提供します。

AWSServiceRoleForUserSubscriptions は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 25 日 16:14 UTC
- 編集日時: 2024 年 4 月 25 日 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
"Sid" : "SubscriptionManagementPolicy",
"Effect" : "Allow",
"Action" : [
  "identitystore:DescribeGroup",
  "identitystore:DescribeUser",
  "identitystore:IsMemberInGroups",
  "identitystore:ListGroupMemberships",
  "organizations:DescribeOrganization",
  "sso:DescribeApplication",
  "sso:DescribeInstance",
  "sso:ListInstances"
],
"Resource" : [
  "*"
]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRolePolicyForBackupReports

説明：ユーザーに代わってコンプライアンスレポートを作成するための AWS Backup アクセス許可を付与します

AWSServiceRolePolicyForBackupReports は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2021 年 8 月 19 日 21:16 UTC
- 編集日時: 2023 年 3 月 10 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSServiceRolePolicyForBackupRestoreTesting

説明：このポリシーには、復元をテストするためのアクセス許可と、テスト中に作成されたリソースをクリーンアップするためのアクセス許可が含まれています。

AWSServiceRolePolicyForBackupRestoreTesting は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 10 日 23:37 UTC
- 編集日時: 2024 年 2 月 14 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSShieldDRTAccessPolicy

説明: 重要度の高いイベント中の AWS DDoS 攻撃の軽減を支援する AWS アカウント ために、DDoS レスポンスチームに への制限付きアクセスを提供します。

AWSShieldDRTAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSShieldDRTAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 6 月 5 日 22:29 UTC
- 編集日時: 2020 年 12 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSShieldServiceRolePolicy

説明： AWS Shield がユーザーに代わって AWS リソースにアクセスして DDoS 保護を提供できるようにします。

AWSShieldServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 11 月 17 日 19:17 UTC
- 編集日時: 2021 年 11 月 17 日 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSSMForSAPServiceLinkedRolePolicy

説明： SAP ソフトウェアを管理および統合するために必要なアクセス許可を AWS Systems Manager for SAP に提供します AWS。

AWSSSMForSAPServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 16 日 01:18 UTC
- 編集日時: 2024 年 4 月 11 日 18:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
```

```
"Action" : [
  "events:DeleteRule",
  "events:PutTargets",
  "events:DescribeRule",
  "events:PutRule",
  "events:RemoveTargets"
],
"Resource" : [
  "arn:*:events:*:*:rule/SSMSAPManagedRule*",
  "arn:*:events:*:*:event-bus/default"
]
},
{
  "Sid" : "DocumentActions",
  "Effect" : "Allow",
  "Action" : [
    "ssm:DescribeDocument",
    "ssm:SendCommand"
  ],
  "Resource" : [
    "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
    "arn:*:ssm:*:*:document/AWSSSMSAP*",
    "arn:*:ssm:*:*:document/AWSSAP*"
  ]
},
{
  "Sid" : "CustomerSendCommand",
  "Effect" : "Allow",
  "Action" : "ssm:SendCommand",
  "Resource" : "arn:*:ec2:*:*:instance/*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "ssm:resourceTag/SSMForSAPManaged" : "True"
    }
  }
},
{
  "Sid" : "InstanceTagActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : "arn:*:ec2:*:*:instance/*",
```

```
"Condition" : {
  "Null" : {
    "aws:RequestTag/awsApplication" : "false"
  },
  "StringEqualsIgnoreCase" : {
    "ec2:ResourceTag/SSMForSAPManaged" : "True"
  }
},
{
  "Sid" : "DescribeTag",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeTags",
  "Resource" : "*"
},
{
  "Sid" : "GetApplication",
  "Effect" : "Allow",
  "Action" : "servicecatalog:GetApplication",
  "Resource" : "arn:*:servicecatalog:*:*:*"
},
{
  "Sid" : "UpdateOrDeleteApplication",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:DeleteApplication",
    "servicecatalog:UpdateApplication"
  ],
  "Resource" : "arn:*:servicecatalog:*:*:*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "CreateApplication",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:TagResource",
    "servicecatalog:CreateApplication"
  ],
  "Resource" : "arn:*:servicecatalog:*:*:*",
  "Condition" : {
```

```
    "StringEquals" : {
      "aws:RequestTag/SSMForSAPCreated" : "True"
    }
  },
  {
    "Sid" : "CreateServiceLinkedRole",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:*:iam:*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "PutMetricData",
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage",
          "AWS/SSMForSAP"
        ]
      }
    }
  },
  {
    "Sid" : "CreateAttributeGroup",
    "Effect" : "Allow",
    "Action" : "servicecatalog:CreateAttributeGroup",
    "Resource" : "arn*:servicecatalog:*:*/attribute-groups/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/SSMForSAPCreated" : "True"
      }
    }
  },
  {
    "Sid" : "GetAttributeGroup",
```

```
"Effect" : "Allow",
"Action" : "servicecatalog:GetAttributeGroup",
"Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
},
{
  "Sid" : "DeleteAttributeGroup",
  "Effect" : "Allow",
  "Action" : "servicecatalog:DeleteAttributeGroup",
  "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "AttributeGroupActions",
  "Effect" : "Allow",
  "Action" : [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
  ],
  "Resource" : "arn:*:servicecatalog:*:*:*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "ListAssociatedAttributeGroups",
  "Effect" : "Allow",
  "Action" : "servicecatalog:ListAssociatedAttributeGroups",
  "Resource" : "arn:*:servicecatalog:*:*:*"
},
{
  "Sid" : "CreateGroup",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:CreateGroup",
    "resource-groups:Tag"
  ],
  "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
  "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "SSMForSAPCreated"
      ]
    }
  }
},
{
  "Sid" : "GetGroup",
  "Effect" : "Allow",
  "Action" : "resource-groups:GetGroup",
  "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
},
{
  "Sid" : "DeleteGroup",
  "Effect" : "Allow",
  "Action" : "resource-groups:DeleteGroup",
  "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/SSMForSAPCreated" : "True"
    }
  }
},
{
  "Sid" : "CreateAppTagResourceGroup",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:CreateGroup"
  ],
  "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
    }
  }
},
{
  "Sid" : "TagAppTagResourceGroup",
  "Effect" : "Allow",
  "Action" : [
```

```
    "resource-groups:Tag"
  ],
  "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
    }
  }
},
{
  "Sid" : "GetAppTagResourceGroupConfig",
  "Effect" : "Allow",
  "Action" : [
    "resource-groups:GetGroupConfiguration"
  ],
  "Resource" : [
    "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
  ]
},
{
  "Sid" : "StartStopInstances",
  "Effect" : "Allow",
  "Action" : [
    "ec2:StartInstances",
    "ec2:StopInstances"
  ],
  "Resource" : "arn:*:ec2:*:*:instance/*",
  "Condition" : {
    "StringEqualsIgnoreCase" : {
      "ec2:resourceTag/SSMForSAPManaged" : "True"
    }
  }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSSMOpsInsightsServiceRolePolicy

説明: サービスにリンクされたロールのポリシー AWSServiceRoleForAmazonSSM_OpsInsights

AWSSSMOpsInsightsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 6 月 16 日 20:12 UTC
- 編集日時: 2021 年 6 月 16 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSSODirectoryAdministrator

説明: SSO ディレクトリの管理者アクセス

AWSSSODirectoryAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSODirectoryAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 31 日 23:54 UTC
- 編集日時: 2022 年 10 月 20 日 20:34 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSSODirectoryReadOnly

説明: SSO ディレクトリの ReadOnly アクセス

AWSSSODirectoryReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSODirectoryReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 10 月 31 日 23:49 UTC
- 編集日時: 2022 年 11 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

```
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSSOMasterAccountAdministrator

説明： Organizations のマスターアカウントとメンバーアカウント、およびクラウドアプリケーションを管理するための AWS SSO AWS 内のアクセスを提供します

AWSSSOMasterAccountAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOMasterAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:36 UTC
- 編集日時: 2024 年 4 月 26 日 00:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
```

```
    "organizations:DescribeOrganization",
    "organizations:ListChildren",
    "organizations:DescribeAccount",
    "organizations:ListParents",
    "organizations:ListDelegatedAdministrators",
    "sso:*",
    "sso-directory:*",
    "identitystore:*",
    "identitystore-auth:*",
    "ds:CreateAlias",
    "access-analyzer:ValidatePolicy",
    "signin:CreateTrustedIdentityPropagationApplicationForConsole",
    "signin:ListTrustedIdentityPropagationApplicationsForConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSSSOManageDelegatedAdministrator",
  "Effect" : "Allow",
  "Action" : [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "sso.amazonaws.com"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSSOMemberAccountAdministrator

説明： Organizations メンバーアカウントとクラウドアプリケーションを管理するための AWS SSO AWS 内のアクセスを提供します

AWSSSOMemberAccountAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOMemberAccountAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:45 UTC
- 編集日時: 2024 年 4 月 26 日 00:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
```



```
    "iam:ListPolicies",
    "organizations:EnableAWSServiceAccess",
    "organizations:DescribeOrganization",
    "organizations:DescribeAccount",
    "organizations:ListRoots",
    "organizations:ListAccounts",
    "organizations:ListAccountsForParent",
    "organizations:ListParents",
    "organizations:ListChildren",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListDelegatedAdministrators",
    "sso:*",
    "sso-directory:*",
    "identitystore:*",
    "identitystore-auth:*",
    "ds:CreateAlias",
    "access-analyzer:ValidatePolicy",
    "signin:CreateTrustedIdentityPropagationApplicationForConsole",
    "signin:ListTrustedIdentityPropagationApplicationsForConsole"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSSSOManageDelegatedAdministrator",
  "Effect" : "Allow",
  "Action" : [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "organizations:ServicePrincipal" : "sso.amazonaws.com"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSSOReadOnly

説明： AWS SSO 設定への読み取り専用アクセスを提供します。

AWSSSOReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSSOReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 27 日 20:24 UTC
- 編集日時: 2024 年 4 月 26 日 00:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
```

```
"Action" : [
  "ds:DescribeDirectories",
  "ds:DescribeTrusts",
  "iam:ListPolicies",
  "organizations:DescribeOrganization",
  "organizations:DescribeAccount",
  "organizations:ListParents",
  "organizations:ListChildren",
  "organizations:ListAccounts",
  "organizations:ListRoots",
  "organizations:ListAccountsForParent",
  "organizations:ListOrganizationalUnitsForParent",
  "organizations:ListDelegatedAdministrators",
  "sso:Describe*",
  "sso:Get*",
  "sso:List*",
  "sso:Search*",
  "sso-directory:DescribeDirectory",
  "access-analyzer:ValidatePolicy",
  "signin:ListTrustedIdentityPropagationApplicationsForConsole"
],
"Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSSOServiceRolePolicy

説明：ユーザーに代わって IAM ロール、ポリシー、SAML IdP などの AWS リソースを管理するための AWS SSO アクセス許可を付与します。

AWSSSOServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 5 日 18:36 UTC
- 編集日時: 2022 年 10 月 20 日 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSS0ServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v17 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
    "*"
  ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSStepFunctionsConsoleFullAccess

説明：ユーザー/ロールなどに AWS StepFunctions コンソールへのアクセスを提供するアクセスポリシー。完全なコンソールエクスペリエンスを実現するには、このポリシーに加えて、サービスが引き受けることができる他の IAM ロールに対して iam:PassRole permission が必要になる場合があります。

AWSStepFunctionsConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStepFunctionsConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:54 UTC
- 編集日時: 2017 年 1 月 12 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```



```
"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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSStepFunctionsFullAccess

説明： AWS StepFunctions API へのユーザー/ロール/その他アクセスを提供するアクセスポリシー。フルアクセスの場合、このポリシーに加えて、ユーザーは、サービスが引き受けることができる少なくとも 1 つの IAM ロールに対して iam:PassRole permission を持っている必要があります。

AWSStepFunctionsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSStepFunctionsFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:51 UTC
- 編集日時: 2017 年 1 月 11 日 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSStepFunctionsReadOnlyAccess

説明：ユーザー/ロールなどに AWS StepFunctions サービスへの読み取り専用アクセスを提供するアクセスポリシー。

AWSStepFunctionsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStepFunctionsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 1 月 11 日 21:46 UTC
- 編集日時: 2024 年 4 月 26 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
```

```
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:DescribeActivity",
    "states:ListTagsForResource",
    "states:DescribeMapRun",
    "states:ListMapRuns",
    "states:DescribeStateMachineAlias",
    "states:ListStateMachineAliases",
    "states:ListStateMachineVersions",
    "states:ValidateStateMachineDefinition"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSStorageGatewayFullAccess

説明： 経由で AWS Storage Gateway へのフルアクセスを提供します AWS Management Console。

AWSStorageGatewayFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStorageGatewayFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2022 年 9 月 6 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSStorageGatewayReadOnlyAccess

説明： 経由で AWS Storage Gateway へのアクセスを提供します AWS Management Console。

AWSStorageGatewayReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSStorageGatewayReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2022 年 9 月 6 日 20:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSStorageGatewayServiceRolePolicy

説明： AWS Storage Gateway が他の サービスと Storage Gateway との統合を可能にするために使用する AWS サービスにリンクされたロール Storage Gateway。

AWSStorageGatewayServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 2 月 17 日 19:03 UTC
- 編集日時: 2021 年 2 月 17 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSupplyChainFederationAdminAccess

説明: AWS Supply Chain アプリケーション内でアクションを実行するために必要なアクセス許可を含め、Supply Chain AWS フェデレーテッドユーザーに Supply Chain AWS アプリケーションへのアクセス AWSSupplyChainFederationAdminAccess を提供します。このポリシーは、IAM Identity Center のユーザーとグループに対する管理アクセス許可を提供し、ユーザーに代わって AWS Supply Chain によって作成されたロールにアタッチされます。他の IAM エンティティに AWSSupplyChainFederationAdminAccess ポリシーをアタッチしないでください。

AWSSupplyChainFederationAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupplyChainFederationAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 3 月 1 日 18:54 UTC
- 編集日時: 2023 年 11 月 1 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
```

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSupportAccess

説明：ユーザーが AWS Support センターにアクセスできるようにします。

AWSSupportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSupportAppFullAccess

説明 : AWS Support アプリおよび AWS Support や Service Quotas などのその他の必要なサービスへのフルアクセスを提供します。このポリシーには、ユーザーがサポートケース AWS Support のに連絡したり、サービスクォータを変更したり、関連するサービスにリンクされたロールを作成したりできるように、サポートサービスを使用するアクセス許可が含まれています。

AWSSupportAppFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAppFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2022 年 8 月 22 日 16:53 UTC
- 編集日時: 2022 年 8 月 22 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSupportAppReadOnlyAccess

説明： AWS Support アプリへの読み取り専用アクセスを提供します。

AWSSupportAppReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportAppReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 22 日 17:01 UTC
- 編集日時: 2022 年 8 月 22 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSupportPlansFullAccess

説明： サポートプランへのフルアクセスを提供します。

AWSSupportPlansFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 27 日 18:19 UTC
- 編集日時: 2023 年 5 月 9 日 21:07 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSupportPlansReadOnlyAccess

説明： サポートプランへの読み取り専用アクセスを提供します。

AWSSupportPlansReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSupportPlansReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 9 月 27 日 18:08 UTC
- 編集日時: 2022 年 9 月 27 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSSupportServiceRolePolicy

説明 : AWS Support が AWS リソースにアクセスして、請求、管理、サポートサービスを提供できるようにします。

AWSSupportServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 4 月 19 日 18:04 UTC
- 編集日時: 2024 年 5 月 2 日 02:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v36 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
```

```
"Action" : [
  "apigateway:GET"
],
"Effect" : "Allow",
"Resource" : [
  "arn:aws:apigateway:*::/account",
  "arn:aws:apigateway:*::/apis",
  "arn:aws:apigateway:*::/apis/*",
  "arn:aws:apigateway:*::/apis/*/authorizers",
  "arn:aws:apigateway:*::/apis/*/authorizers/*",
  "arn:aws:apigateway:*::/apis/*/deployments",
  "arn:aws:apigateway:*::/apis/*/deployments/*",
  "arn:aws:apigateway:*::/apis/*/integrations",
  "arn:aws:apigateway:*::/apis/*/integrations/*",
  "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
  "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
  "arn:aws:apigateway:*::/apis/*/models",
  "arn:aws:apigateway:*::/apis/*/models/*",
  "arn:aws:apigateway:*::/apis/*/routes",
  "arn:aws:apigateway:*::/apis/*/routes/*",
  "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
  "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
  "arn:aws:apigateway:*::/apis/*/stages",
  "arn:aws:apigateway:*::/apis/*/stages/*",
  "arn:aws:apigateway:*::/clientcertificates",
  "arn:aws:apigateway:*::/clientcertificates/*",
  "arn:aws:apigateway:*::/domainnames",
  "arn:aws:apigateway:*::/domainnames/*",
  "arn:aws:apigateway:*::/domainnames/*/apimappings",
  "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
  "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
  "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
  "arn:aws:apigateway:*::/restapis",
  "arn:aws:apigateway:*::/restapis/*",
  "arn:aws:apigateway:*::/restapis/*/authorizers",
  "arn:aws:apigateway:*::/restapis/*/authorizers/*",
  "arn:aws:apigateway:*::/restapis/*/deployments",
  "arn:aws:apigateway:*::/restapis/*/deployments/*",
  "arn:aws:apigateway:*::/restapis/*/models",
  "arn:aws:apigateway:*::/restapis/*/models/*",
  "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
  "arn:aws:apigateway:*::/restapis/*/resources",
  "arn:aws:apigateway:*::/restapis/*/resources/*",
```

```

    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
    *",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
    "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
    "arn:aws:apigateway:*::/restapis/*/stages",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/usageplans",
    "arn:aws:apigateway:*::/usageplans/*",
    "arn:aws:apigateway:*::/vpclinks",
    "arn:aws:apigateway:*::/vpclinks/*"
  ]
},
{
  "Sid" : "AWSSupportDeleteRoleAccess",
  "Action" : [
    "iam:DeleteRole"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "arn:aws:iam:*::role/aws-service-role/support.amazonaws.com/
    AWSServiceRoleForSupport"
  ]
},
{
  "Sid" : "AWSSupportActions",
  "Action" : [
    "access-analyzer:getAccessPreview",
    "access-analyzer:getAnalyzedResource",
    "access-analyzer:getAnalyzer",
    "access-analyzer:getArchiveRule",
    "access-analyzer:getFinding",
    "access-analyzer:getGeneratedPolicy",
    "access-analyzer:listAccessPreviewFindings",
    "access-analyzer:listAccessPreviews",
    "access-analyzer:listAnalyzedResources",
    "access-analyzer:listAnalyzers",
    "access-analyzer:listArchiveRules",
    "access-analyzer:listFindings",
    "access-analyzer:listPolicyGenerations",
    "acm-pca:describeCertificateAuthority",
    "acm-pca:describeCertificateAuthorityAuditReport",
    "acm-pca:getCertificate",

```



```
"acm-pca:getCertificateAuthorityCertificate",
"acm-pca:getCertificateAuthorityCsr",
"acm-pca:listCertificateAuthorities",
"acm-pca:listTags",
"acm:describeCertificate",
"acm:getAccountConfiguration",
"acm:getCertificate",
"acm:listCertificates",
"acm:listTagsForCertificate",
"airflow:getEnvironment",
"airflow:listEnvironments",
"airflow:listTagsForResource",
"amplify:getApp",
"amplify:getBackendEnvironment",
"amplify:getBranch",
"amplify:getDomainAssociation",
"amplify:getJob",
"amplify:getWebhook",
"amplify:listApps",
"amplify:listBackendEnvironments",
"amplify:listBranches",
"amplify:listDomainAssociations",
"amplify:listWebhooks",
"amplifyuibuilder:exportComponents",
"amplifyuibuilder:exportThemes",
"appflow:describeConnectorEntity",
"appflow:describeConnectorProfiles",
"appflow:describeConnectors",
"appflow:describeFlow",
"appflow:describeFlowExecutionRecords",
"appflow:listConnectorEntities",
"appflow:listFlows",
"application-autoscaling:describeScalableTargets",
"application-autoscaling:describeScalingActivities",
"application-autoscaling:describeScalingPolicies",
"application-autoscaling:describeScheduledActions",
"applicationinsights:describeApplication",
"applicationinsights:describeComponent",
"applicationinsights:describeComponentConfiguration",
"applicationinsights:describeComponentConfigurationRecommendation",
"applicationinsights:describeLogPattern",
"applicationinsights:describeObservation",
"applicationinsights:describeProblem",
"applicationinsights:describeProblemObservations",
```

```
"applicationinsights:listApplications",
"applicationinsights:listComponents",
"applicationinsights:listConfigurationHistory",
"applicationinsights:listLogPatterns",
"applicationinsights:listLogPatternSets",
"applicationinsights:listProblems",
"appmesh:describeGatewayRoute",
"appmesh:describeMesh",
"appmesh:describeRoute",
"appmesh:describeVirtualGateway",
"appmesh:describeVirtualNode",
"appmesh:describeVirtualRouter",
"appmesh:describeVirtualService",
"appmesh:listGatewayRoutes",
"appmesh:listMeshes",
"appmesh:listRoutes",
"appmesh:listTagsForResource",
"appmesh:listVirtualGateways",
"appmesh:listVirtualNodes",
"appmesh:listVirtualRouters",
"appmesh:listVirtualServices",
"apprunner:describeAutoScalingConfiguration",
"apprunner:describeCustomDomains",
"apprunner:describeOperation",
"apprunner:describeService",
"apprunner:listAutoScalingConfigurations",
"apprunner:listConnections",
"apprunner:listOperations",
"apprunner:listServices",
"apprunner:listTagsForResource",
"appstream:describeAppBlockBuilderAppBlockAssociations",
"appstream:describeAppBlockBuilders",
"appstream:describeAppBlocks",
"appstream:describeApplicationFleetAssociations",
"appstream:describeApplications",
"appstream:describeDirectoryConfigs",
"appstream:describeEntitlements",
"appstream:describeFleets",
"appstream:describeImageBuilders",
"appstream:describeImagePermissions",
"appstream:describeImages",
"appstream:describeSessions",
"appstream:describeStacks",
"appstream:describeUsageReportSubscriptions",
```

```
"appstream:describeUsers",
"appstream:describeUserStackAssociations",
"appstream:listAssociatedFleets",
"appstream:listAssociatedStacks",
"appstream:listEntitledApplications",
"appstream:listTagsForResource",
"appsync:getApiAssociation",
"appsync:getApiCache",
"appsync:getDomainName",
"appsync:getFunction",
"appsync:getGraphQLApi",
"appsync:getIntrospectionSchema",
"appsync:getResolver",
"appsync:getSchemaCreationStatus",
"appsync:getSourceApiAssociation",
"appsync:getType",
"appsync:listDataSources",
"appsync:listDomainNames",
"appsync:listFunctions",
"appsync:listGraphQLApis",
"appsync:listResolvers",
"appsync:listResolversByFunction",
"appsync:listSourceApiAssociations",
"appsync:listTypes",
"appsync:listTypesByAssociation",
"aps:describeAlertManagerDefinition",
"aps:describeRuleGroupsNamespace",
"aps:describeScraper",
"aps:describeWorkspace",
"aps:listRuleGroupsNamespaces",
"aps:listScrapers",
"aps:listWorkspaces",
"athena:batchGetNamedQuery",
"athena:batchGetQueryExecution",
"athena:getCalculationExecution",
"athena:getCalculationExecutionStatus",
"athena:getDataCatalog",
"athena:getNamedQuery",
"athena:getNotebookMetadata",
"athena:getQueryExecution",
"athena:getQueryRuntimeStatistics",
"athena:getSession",
"athena:getSessionStatus",
"athena:getWorkGroup",
```

```
"athena:listApplicationDPUSizes",
"athena:listCalculationExecutions",
"athena:listDataCatalogs",
"athena:listEngineVersions",
"athena:listExecutors",
"athena:listNamedQueries",
"athena:listNotebookMetadata",
"athena:listNotebookSessions",
"athena:listQueryExecutions",
"athena:listSessions",
"athena:listTagsForResource",
"athena:listWorkGroups",
"auditmanager:getAccountStatus",
"auditmanager:getDelegations",
"auditmanager:listAssessmentFrameworks",
"auditmanager:listAssessmentReports",
"auditmanager:listAssessments",
"auditmanager:listControls",
"auditmanager:listKeywordsForDataSource",
"auditmanager:listNotifications",
"autoscaling-plans:describeScalingPlanResources",
"autoscaling-plans:describeScalingPlans",
"autoscaling-plans:getScalingPlanResourceForecastData",
"autoscaling:describeAccountLimits",
"autoscaling:describeAdjustmentTypes",
"autoscaling:describeAutoScalingGroups",
"autoscaling:describeAutoScalingInstances",
"autoscaling:describeAutoScalingNotificationTypes",
"autoscaling:describeInstanceRefreshes",
"autoscaling:describeLaunchConfigurations",
"autoscaling:describeLifecycleHooks",
"autoscaling:describeLifecycleHookTypes",
"autoscaling:describeLoadBalancers",
"autoscaling:describeLoadBalancerTargetGroups",
"autoscaling:describeMetricCollectionTypes",
"autoscaling:describeNotificationConfigurations",
"autoscaling:describePolicies",
"autoscaling:describeScalingActivities",
"autoscaling:describeScalingProcessTypes",
"autoscaling:describeScheduledActions",
"autoscaling:describeTags",
"autoscaling:describeTerminationPolicyTypes",
"autoscaling:describeWarmPool",
"backup:describeBackupJob",
```

```
"backup:describeBackupVault",
"backup:describeCopyJob",
"backup:describeFramework",
"backup:describeGlobalSettings",
"backup:describeProtectedResource",
"backup:describeRecoveryPoint",
"backup:describeRegionSettings",
"backup:describeReportJob",
"backup:describeReportPlan",
"backup:describeRestoreJob",
"backup:getBackupPlan",
"backup:getBackupPlanFromJSON",
"backup:getBackupPlanFromTemplate",
"backup:getBackupSelection",
"backup:getBackupVaultAccessPolicy",
"backup:getBackupVaultNotifications",
"backup:getLegalHold",
"backup:getRecoveryPointRestoreMetadata",
"backup:getRestoreJobMetadata",
"backup:getRestoreTestingInferredMetadata",
"backup:getRestoreTestingPlan",
"backup:getRestoreTestingSelection",
"backup:getSupportedResourceTypes",
"backup:listBackupJobs",
"backup:listBackupPlans",
"backup:listBackupPlanTemplates",
"backup:listBackupPlanVersions",
"backup:listBackupSelections",
"backup:listBackupVaults",
"backup:listCopyJobs",
"backup:listFrameworks",
"backup:listLegalHolds",
"backup:listProtectedResources",
"backup:listRecoveryPointsByBackupVault",
"backup:listRecoveryPointsByLegalHold",
"backup:listRecoveryPointsByResource",
"backup:listReportJobs",
"backup:listReportPlans",
"backup:listRestoreJobs",
"backup:listRestoreJobsByProtectedResource",
"backup:listRestoreTestingPlans",
"backup:listRestoreTestingSelections",
"backup:listTags",
"backup-gateway:getGateway",
```

```
"backup-gateway:getHypervisor",
"backup-gateway:getHypervisorPropertyMappings",
"backup-gateway:getVirtualMachine",
"backup-gateway:listGateways",
"backup-gateway:listHypervisors",
"backup-gateway:listVirtualMachines",
"batch:describeComputeEnvironments",
"batch:describeJobDefinitions",
"batch:describeJobQueues",
"batch:describeJobs",
"batch:listJobs",
"braket:getDevice",
"braket:getQuantumTask",
"braket:searchDevices",
"braket:searchQuantumTasks",
"budgets:viewBudget",
"ce:getCostAndUsage",
"ce:getCostAndUsageWithResources",
"ce:getCostForecast",
"ce:getDimensionValues",
"ce:getReservationCoverage",
"ce:getReservationPurchaseRecommendation",
"ce:getReservationUtilization",
"ce:getRightsizingRecommendation",
"ce:getSavingsPlansCoverage",
"ce:getSavingsPlansPurchaseRecommendation",
"ce:getSavingsPlansUtilization",
"ce:getSavingsPlansUtilizationDetails",
"ce:getTags",
"chime:describeAppInstance",
"chime:getAttendee",
"chime:getGlobalSettings",
"chime:getMediaCapturePipeline",
"chime:getMediaPipeline",
"chime:getMeeting",
"chime:getProxySession",
"chime:getSipMediaApplication",
"chime:getSipRule",
"chime:getVoiceConnector",
"chime:getVoiceConnectorGroup",
"chime:getVoiceConnectorLoggingConfiguration",
"chime:listAppInstances",
"chime:listAttendees",
"chime:listChannelBans",
```

```
"chime:listChannels",
"chime:listChannelsModeratedByAppInstanceUser",
"chime:listMediaCapturePipelines",
"chime:listMediaPipelines",
"chime:listMeetings",
"chime:listSipMediaApplications",
"chime:listSipRules",
"chime:listVoiceConnectorGroups",
"chime:listVoiceConnectors",
"cleanrooms:batchGetCollaborationAnalysisTemplate",
"cleanrooms:batchGetSchema",
"cleanrooms:getAnalysisTemplate",
"cleanrooms:getCollaboration",
"cleanrooms:getCollaborationAnalysisTemplate",
"cleanrooms:getConfiguredTable",
"cleanrooms:getConfiguredTableAssociation",
"cleanrooms:getMembership",
"cleanrooms:getSchema",
"cleanrooms:listAnalysisTemplates",
"cleanrooms:listCollaborationAnalysisTemplates",
"cleanrooms:listCollaborations",
"cleanrooms:listConfiguredTableAssociations",
"cleanrooms:listConfiguredTables",
"cleanrooms:listMembers",
"cleanrooms:listMemberships",
"cleanrooms:listSchemas",
"cloud9:describeEnvironmentMemberships",
"cloud9:describeEnvironments",
"cloud9:listEnvironments",
"clouddirectory:getDirectory",
"clouddirectory:listDirectories",
"cloudformation:batchDescribeTypeConfigurations",
"cloudformation:describeAccountLimits",
"cloudformation:describeChangeSet",
"cloudformation:describeChangeSetHooks",
"cloudformation:describePublisher",
"cloudformation:describeStackEvents",
"cloudformation:describeStackInstance",
"cloudformation:describeStackResource",
"cloudformation:describeStackResources",
"cloudformation:describeStacks",
"cloudformation:describeStackSet",
"cloudformation:describeStackSetOperation",
"cloudformation:describeType",
```

```
"cloudformation:describeTypeRegistration",
"cloudformation:estimateTemplateCost",
"cloudformation:getStackPolicy",
"cloudformation:getTemplate",
"cloudformation:getTemplateSummary",
"cloudformation:listChangeSets",
"cloudformation:listExports",
"cloudformation:listImports",
"cloudformation:listStackInstances",
"cloudformation:listStackResources",
"cloudformation:listStacks",
"cloudformation:listStackSetOperationResults",
"cloudformation:listStackSetOperations",
"cloudformation:listStackSets",
"cloudformation:listTypeRegistrations",
"cloudformation:listTypes",
"cloudformation:listTypeVersions",
"cloudfront:describeFunction",
"cloudfront:getCachePolicy",
"cloudfront:getCachePolicyConfig",
"cloudfront:getCloudFrontOriginAccessIdentity",
"cloudfront:getCloudFrontOriginAccessIdentityConfig",
"cloudfront:getContinuousDeploymentPolicy",
"cloudfront:getContinuousDeploymentPolicyConfig",
"cloudfront:getDistribution",
"cloudfront:getDistributionConfig",
"cloudfront:getInvalidation",
"cloudfront:getKeyGroup",
"cloudfront:getKeyGroupConfig",
"cloudfront:getMonitoringSubscription",
"cloudfront:getOriginAccessControl",
"cloudfront:getOriginAccessControlConfig",
"cloudfront:getOriginRequestPolicy",
"cloudfront:getOriginRequestPolicyConfig",
"cloudfront:getPublicKey",
"cloudfront:getPublicKeyConfig",
"cloudfront:getRealtimeLogConfig",
"cloudfront:getResponseHeadersPolicy",
"cloudfront:getResponseHeadersPolicyConfig",
"cloudfront:getStreamingDistribution",
"cloudfront:getStreamingDistributionConfig",
"cloudfront:listCachePolicies",
"cloudfront:listCloudFrontOriginAccessIdentities",
"cloudfront:listContinuousDeploymentPolicies",
```



```
"cloudfront:listDistributions",
"cloudfront:listDistributionsByCachePolicyId",
"cloudfront:listDistributionsByKeyGroup",
"cloudfront:listDistributionsByOriginRequestPolicyId",
"cloudfront:listDistributionsByRealtimeLogConfig",
"cloudfront:listDistributionsByResponseHeadersPolicyId",
"cloudfront:listDistributionsByWebACLId",
"cloudfront:listFunctions",
"cloudfront:listInvalidations",
"cloudfront:listKeyGroups",
"cloudfront:listOriginAccessControls",
"cloudfront:listOriginRequestPolicies",
"cloudfront:listPublicKeys",
"cloudfront:listRealtimeLogConfigs",
"cloudfront:listResponseHeadersPolicies",
"cloudfront:listStreamingDistributions",
"cloudhsm:describeBackups",
"cloudhsm:describeClusters",
"cloudsearch:describeAnalysisSchemes",
"cloudsearch:describeAvailabilityOptions",
"cloudsearch:describeDomains",
"cloudsearch:describeExpressions",
"cloudsearch:describeIndexFields",
"cloudsearch:describeScalingParameters",
"cloudsearch:describeServiceAccessPolicies",
"cloudsearch:describeSuggesters",
"cloudsearch:listDomainNames",
"cloudtrail:describeTrails",
"cloudtrail:getEventSelectors",
"cloudtrail:getInsightSelectors",
"cloudtrail:getTrail",
"cloudtrail:getTrailStatus",
"cloudtrail:listPublicKeys",
"cloudtrail:listTags",
"cloudtrail:listTrails",
"cloudtrail:lookupEvents",
"cloudwatch:describeAlarmHistory",
"cloudwatch:describeAlarms",
"cloudwatch:describeAlarmsForMetric",
"cloudwatch:describeAnomalyDetectors",
"cloudwatch:describeInsightRules",
"cloudwatch:getDashboard",
"cloudwatch:getInsightRuleReport",
"cloudwatch:getMetricData",
```

```
"cloudwatch:getMetricStatistics",
"cloudwatch:getMetricStream",
"cloudwatch:listDashboards",
"cloudwatch:listManagedInsightRules",
"cloudwatch:listMetrics",
"cloudwatch:listMetricStreams",
"codeartifact:describeDomain",
"codeartifact:describePackageVersion",
"codeartifact:describeRepository",
"codeartifact:getDomainPermissionsPolicy",
"codeartifact:getRepositoryEndpoint",
"codeartifact:getRepositoryPermissionsPolicy",
"codeartifact:listDomains",
"codeartifact:listPackages",
"codeartifact:listPackageVersionAssets",
"codeartifact:listPackageVersions",
"codeartifact:listRepositories",
"codeartifact:listRepositoriesInDomain",
"codebuild:batchGetBuildBatches",
"codebuild:batchGetBuilds",
"codebuild:batchGetFleets",
"codebuild:batchGetProjects",
"codebuild:listBuildBatches",
"codebuild:listBuildBatchesForProject",
"codebuild:listBuilds",
"codebuild:listBuildsForProject",
"codebuild:listCuratedEnvironmentImages",
"codebuild:listFleets",
"codebuild:listProjects",
"codebuild:listSourceCredentials",
"codecommit:batchGetRepositories",
"codecommit:getBranch",
"codecommit:getRepository",
"codecommit:getRepositoryTriggers",
"codecommit:listBranches",
"codecommit:listRepositories",
"codedeploy:batchGetApplicationRevisions",
"codedeploy:batchGetApplications",
"codedeploy:batchGetDeploymentGroups",
"codedeploy:batchGetDeploymentInstances",
"codedeploy:batchGetDeployments",
"codedeploy:batchGetDeploymentTargets",
"codedeploy:batchGetOnPremisesInstances",
"codedeploy:getApplication",
```

```
"codedeploy:getApplicationRevision",
"codedeploy:getDeployment",
"codedeploy:getDeploymentConfig",
"codedeploy:getDeploymentGroup",
"codedeploy:getDeploymentInstance",
"codedeploy:getDeploymentTarget",
"codedeploy:getOnPremisesInstance",
"codedeploy:listApplicationRevisions",
"codedeploy:listApplications",
"codedeploy:listDeploymentConfigs",
"codedeploy:listDeploymentGroups",
"codedeploy:listDeploymentInstances",
"codedeploy:listDeployments",
"codedeploy:listDeploymentTargets",
"codedeploy:listGitHubAccountTokenNames",
"codedeploy:listOnPremisesInstances",
"codepipeline:getJobDetails",
"codepipeline:getPipeline",
"codepipeline:getPipelineExecution",
"codepipeline:getPipelineState",
"codepipeline:listActionExecutions",
"codepipeline:listActionTypes",
"codepipeline:listPipelineExecutions",
"codepipeline:listPipelines",
"codepipeline:listWebhooks",
"codestar:describeProject",
"codestar:listProjects",
"codestar:listResources",
"codestar:listTeamMembers",
"codestar:listUserProfiles",
"codestar-connections:getConnection",
"codestar-connections:getHost",
"codestar-connections:listConnections",
"codestar-connections:listHosts",
"cognito-identity:describeIdentityPool",
"cognito-identity:getIdentityPoolRoles",
"cognito-identity:listIdentities",
"cognito-identity:listIdentityPools",
"cognito-idp:describeIdentityProvider",
"cognito-idp:describeResourceServer",
"cognito-idp:describeRiskConfiguration",
"cognito-idp:describeUserImportJob",
"cognito-idp:describeUserPool",
"cognito-idp:describeUserPoolClient",
```

```
"cognito-idp:describeUserPoolDomain",
"cognito-idp:getGroup",
"cognito-idp:getUICustomization",
"cognito-idp:getUserPoolMfaConfig",
"cognito-idp:listGroups",
"cognito-idp:listIdentityProviders",
"cognito-idp:listResourceServers",
"cognito-idp:listUserImportJobs",
"cognito-idp:listUserPoolClients",
"cognito-idp:listUserPools",
"cognito-sync:describeDataset",
"cognito-sync:describeIdentityPoolUsage",
"cognito-sync:describeIdentityUsage",
"cognito-sync:getCognitoEvents",
"cognito-sync:getIdentityPoolConfiguration",
"cognito-sync:listDatasets",
"cognito-sync:listIdentityPoolUsage",
"comprehend:describeDocumentClassificationJob",
"comprehend:describeDocumentClassifier",
"comprehend:describeDominantLanguageDetectionJob",
"comprehend:describeEndpoint",
"comprehend:describeEntitiesDetectionJob",
"comprehend:describeEntityRecognizer",
"comprehend:describeEventsDetectionJob",
"comprehend:describeFlywheel",
"comprehend:describeFlywheelIteration",
"comprehend:describeKeyPhrasesDetectionJob",
"comprehend:describePiiEntitiesDetectionJob",
"comprehend:describeSentimentDetectionJob",
"comprehend:describeTargetedSentimentDetectionJob",
"comprehend:describeTopicsDetectionJob",
"comprehend:listDocumentClassificationJobs",
"comprehend:listDocumentClassifiers",
"comprehend:listDominantLanguageDetectionJobs",
"comprehend:listEndpoints",
"comprehend:listEntitiesDetectionJobs",
"comprehend:listEntityRecognizers",
"comprehend:listEventsDetectionJobs",
"comprehend:listFlywheelIterationHistory",
"comprehend:listFlywheels",
"comprehend:listKeyPhrasesDetectionJobs",
"comprehend:listPiiEntitiesDetectionJobs",
"comprehend:listSentimentDetectionJobs",
"comprehend:listTargetedSentimentDetectionJobs",
```

```
"comprehend:listTopicsDetectionJobs",
"compute-optimizer:getAutoScalingGroupRecommendations",
"compute-optimizer:getEBSVolumeRecommendations",
"compute-optimizer:getEC2InstanceRecommendations",
"compute-optimizer:getEC2RecommendationProjectedMetrics",
"compute-optimizer:getECSServiceRecommendations",
"compute-optimizer:getECSServiceRecommendationProjectedMetrics",
"compute-optimizer:getEnrollmentStatus",
"compute-optimizer:getRecommendationSummaries",
"config:batchGetAggregateResourceConfig",
"config:batchGetResourceConfig",
"config:describeAggregateComplianceByConfigRules",
"config:describeAggregationAuthorizations",
"config:describeComplianceByConfigRule",
"config:describeComplianceByResource",
"config:describeConfigRuleEvaluationStatus",
"config:describeConfigRules",
"config:describeConfigurationAggregators",
"config:describeConfigurationAggregatorSourcesStatus",
"config:describeConfigurationRecorders",
"config:describeConfigurationRecorderStatus",
"config:describeConformancePackCompliance",
"config:describeConformancePacks",
"config:describeConformancePackStatus",
"config:describeDeliveryChannels",
"config:describeDeliveryChannelStatus",
"config:describeOrganizationConfigRules",
"config:describeOrganizationConfigRuleStatuses",
"config:describeOrganizationConformancePacks",
"config:describeOrganizationConformancePackStatuses",
"config:describePendingAggregationRequests",
"config:describeRemediationConfigurations",
"config:describeRemediationExceptions",
"config:describeRemediationExecutionStatus",
"config:describeRetentionConfigurations",
"config:getAggregateComplianceDetailsByConfigRule",
"config:getAggregateConfigRuleComplianceSummary",
"config:getAggregateDiscoveredResourceCounts",
"config:getAggregateResourceConfig",
"config:getComplianceDetailsByConfigRule",
"config:getComplianceDetailsByResource",
"config:getComplianceSummaryByConfigRule",
"config:getComplianceSummaryByResourceType",
"config:getConformancePackComplianceDetails",
```

```
"config:getConformancePackComplianceSummary",
"config:getDiscoveredResourceCounts",
"config:getOrganizationConfigRuleDetailedStatus",
"config:getOrganizationConformancePackDetailedStatus",
"config:getResourceConfigHistory",
"config:listAggregateDiscoveredResources",
"config:listDiscoveredResources",
"config:listTagsForResource",
"connect:describeContact",
"connect:describePhoneNumber",
"connect:describeQuickConnect",
"connect:describeUser",
"connect:getCurrentMetricData",
"connect:getMetricData",
"connect:listContactEvaluations",
"connect:listEvaluationForms",
"connect:listEvaluationFormVersions",
"connect:listPhoneNumbersV2",
"connect:listQuickConnects",
"connect:listRoutingProfiles",
"connect:listSecurityProfiles",
"connect:listUsers",
"connect:listViews",
"connect:listViewVersions",
"controltower:describeAccountFactoryConfig",
"controltower:describeCoreService",
"controltower:describeGuardrail",
"controltower:describeGuardrailForTarget",
"controltower:describeManagedAccount",
"controltower:describeSingleSignOn",
"controltower:getAvailableUpdates",
"controltower:getHomeRegion",
"controltower:getLandingZone",
"controltower:getLandingZoneStatus",
"controltower:listDirectoryGroups",
"controltower:listEnabledControls",
"controltower:listGuardrailsForTarget",
"controltower:listGuardrailViolations",
"controltower:listLandingZones",
"controltower:listManagedAccounts",
"controltower:listManagedAccountsForGuardrail",
"controltower:listManagedAccountsForParent",
"controltower:listManagedOrganizationalUnits",
"controltower:listManagedOrganizationalUnitsForGuardrail",
```

```
"cost-optimization-hub:getPreferences",
"cost-optimization-hub:getRecommendation",
"cost-optimization-hub:listEnrollmentStatuses",
"cost-optimization-hub:listRecommendations",
"cost-optimization-hub:listRecommendationSummaries",
"databrew:describeDataset",
"databrew:describeJob",
"databrew:describeProject",
"databrew:describeRecipe",
"databrew:listDatasets",
"databrew:listJobRuns",
"databrew:listJobs",
"databrew:listProjects",
"databrew:listRecipes",
"databrew:listRecipeVersions",
"databrew:listTagsForResource",
"datapipeline:describeObjects",
"datapipeline:describePipelines",
"datapipeline:getPipelineDefinition",
"datapipeline:listPipelines",
"datapipeline:queryObjects",
"datasync:describeAgent",
"datasync:describeLocationEfs",
"datasync:describeLocationFsxLustre",
"datasync:describeLocationFsxOpenZfs",
"datasync:describeLocationFsxWindows",
"datasync:describeLocationHdfs",
"datasync:describeLocationNfs",
"datasync:describeLocationObjectStorage",
"datasync:describeLocationS3",
"datasync:describeLocationSmb",
"datasync:describeTask",
"datasync:describeTaskExecution",
"datasync:listAgents",
"datasync:listLocations",
"datasync:listTaskExecutions",
"datasync:listTasks",
"dax:describeClusters",
"dax:describeDefaultParameters",
"dax:describeEvents",
"dax:describeParameterGroups",
"dax:describeParameters",
"dax:describeSubnetGroups",
"detective:getMembers",
```

```
"detective:listGraphs",
"detective:listInvitations",
"detective:listMembers",
"devicefarm:getAccountSettings",
"devicefarm:getDevice",
"devicefarm:getDevicePool",
"devicefarm:getDevicePoolCompatibility",
"devicefarm:getJob",
"devicefarm:getProject",
"devicefarm:getRemoteAccessSession",
"devicefarm:getRun",
"devicefarm:getSuite",
"devicefarm:getTest",
"devicefarm:getTestGridProject",
"devicefarm:getTestGridSession",
"devicefarm:getUpload",
"devicefarm:listArtifacts",
"devicefarm:listDevicePools",
"devicefarm:listDevices",
"devicefarm:listJobs",
"devicefarm:listProjects",
"devicefarm:listRemoteAccessSessions",
"devicefarm:listRuns",
"devicefarm:listSamples",
"devicefarm:listSuites",
"devicefarm:listTestGridProjects",
"devicefarm:listTestGridSessionActions",
"devicefarm:listTestGridSessionArtifacts",
"devicefarm:listTestGridSessions",
"devicefarm:listTests",
"devicefarm:listUniqueProblems",
"devicefarm:listUploads",
"directconnect:describeConnectionLoa",
"directconnect:describeConnections",
"directconnect:describeConnectionsOnInterconnect",
"directconnect:describeCustomerMetadata",
"directconnect:describeDirectConnectGatewayAssociationProposals",
"directconnect:describeDirectConnectGatewayAssociations",
"directconnect:describeDirectConnectGatewayAttachments",
"directconnect:describeDirectConnectGateways",
"directconnect:describeHostedConnections",
"directconnect:describeInterconnectLoa",
"directconnect:describeInterconnects",
"directconnect:describeLags",
```



```
"directconnect:describeLoa",
"directconnect:describeLocations",
"directconnect:describeRouterConfiguration",
"directconnect:describeVirtualGateways",
"directconnect:describeVirtualInterfaces",
"dml:getLifecyclePolicies",
"dml:getLifecyclePolicy",
"dms:describeAccountAttributes",
"dms:describeApplicableIndividualAssessments",
"dms:describeConnections",
"dms:describeEndpoints",
"dms:describeEndpointSettings",
"dms:describeEndpointTypes",
"dms:describeEventCategories",
"dms:describeEvents",
"dms:describeEventSubscriptions",
"dms:describeFleetAdvisorCollectors",
"dms:describeFleetAdvisorDatabases",
"dms:describeFleetAdvisorLsaAnalysis",
"dms:describeFleetAdvisorSchemaObjectSummary",
"dms:describeFleetAdvisorSchemas",
"dms:describeOrderableReplicationInstances",
"dms:describePendingMaintenanceActions",
"dms:describeRefreshSchemasStatus",
"dms:describeReplicationInstances",
"dms:describeReplicationInstanceTaskLogs",
"dms:describeReplicationSubnetGroups",
"dms:describeReplicationTaskAssessmentResults",
"dms:describeReplicationTaskAssessmentRuns",
"dms:describeReplicationTaskIndividualAssessments",
"dms:describeReplicationTasks",
"dms:describeSchemas",
"dms:describeTableStatistics",
"docdb-elastic:getCluster",
"docdb-elastic:getClusterSnapshot",
"docdb-elastic:listClusters",
"docdb-elastic:listClusterSnapshots",
"drs:describeJobLogItems",
"drs:describeJobs",
"drs:describeLaunchConfigurationTemplates",
"drs:describeRecoveryInstances",
"drs:describeRecoverySnapshots",
"drs:describeReplicationConfigurationTemplates",
"drs:describeSourceNetworks",
```

```
"drs:describeSourceServers",
"drs:getLaunchConfiguration",
"drs:getReplicationConfiguration",
"drs:listExtensibleSourceServers",
"drs:listLaunchActions",
"drs:listStagingAccounts",
"ds:describeClientAuthenticationSettings",
"ds:describeConditionalForwarders",
"ds:describeDirectories",
"ds:describeDomainControllers",
"ds:describeEventTopics",
"ds:describeLDAPSSettings",
"ds:describeSharedDirectories",
"ds:describeSnapshots",
"ds:describeTrusts",
"ds:getDirectoryLimits",
"ds:getSnapshotLimits",
"ds:listIpRoutes",
"ds:listSchemaExtensions",
"ds:listTagsForResource",
"dynamodb:describeBackup",
"dynamodb:describeContinuousBackups",
"dynamodb:describeContributorInsights",
"dynamodb:describeExport",
"dynamodb:describeGlobalTable",
"dynamodb:describeImport",
"dynamodb:describeKinesisStreamingDestination",
"dynamodb:describeLimits",
"dynamodb:describeStream",
"dynamodb:describeTable",
"dynamodb:describeTimeToLive",
"dynamodb:listBackups",
"dynamodb:listContributorInsights",
"dynamodb:listExports",
"dynamodb:listGlobalTables",
"dynamodb:listImports",
"dynamodb:listStreams",
"dynamodb:listTables",
"dynamodb:listTagsOfResource",
"ec2:describeAccountAttributes",
"ec2:describeAddresses",
"ec2:describeAddressesAttribute",
"ec2:describeAddressTransfers",
"ec2:describeAggregateIdFormat",
```

```
"ec2:describeAvailabilityZones",
"ec2:describeBundleTasks",
"ec2:describeByoipCidrs",
"ec2:describeCapacityReservationFleets",
"ec2:describeCapacityReservations",
"ec2:describeCarrierGateways",
"ec2:describeClassicLinkInstances",
"ec2:describeClientVpnAuthorizationRules",
"ec2:describeClientVpnConnections",
"ec2:describeClientVpnEndpoints",
"ec2:describeClientVpnRoutes",
"ec2:describeClientVpnTargetNetworks",
"ec2:describeCoipPools",
"ec2:describeConversionTasks",
"ec2:describeCustomerGateways",
"ec2:describeDhcpOptions",
"ec2:describeEgressOnlyInternetGateways",
"ec2:describeExportImageTasks",
"ec2:describeExportTasks",
"ec2:describeFastLaunchImages",
"ec2:describeFastSnapshotRestores",
"ec2:describeFleetHistory",
"ec2:describeFleetInstances",
"ec2:describeFleets",
"ec2:describeFlowLogs",
"ec2:describeFpgaImageAttribute",
"ec2:describeFpgaImages",
"ec2:describeHostReservationOfferings",
"ec2:describeHostReservations",
"ec2:describeHosts",
"ec2:describeIamInstanceProfileAssociations",
"ec2:describeIdentityIdFormat",
"ec2:describeIdFormat",
"ec2:describeImageAttribute",
"ec2:describeImages",
"ec2:describeImportImageTasks",
"ec2:describeImportSnapshotTasks",
"ec2:describeInstanceAttribute",
"ec2:describeInstanceCreditSpecifications",
"ec2:describeInstanceEventNotificationAttributes",
"ec2:describeInstanceEventWindows",
"ec2:describeInstances",
"ec2:describeInstanceStatus",
"ec2:describeInstanceTypeOfferings",
```

```
"ec2:describeInstanceTypes",
"ec2:describeInternetGateways",
"ec2:describeIpamPools",
"ec2:describeIpams",
"ec2:describeIpamScopes",
"ec2:describeIpv6Pools",
"ec2:describeKeyPairs",
"ec2:describeLaunchTemplates",
"ec2:describeLaunchTemplateVersions",
"ec2:describeLocalGatewayRouteTables",
"ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:describeLocalGatewayRouteTableVpcAssociations",
"ec2:describeLocalGateways",
"ec2:describeLocalGatewayVirtualInterfaceGroups",
"ec2:describeLocalGatewayVirtualInterfaces",
"ec2:describeManagedPrefixLists",
"ec2:describeMovingAddresses",
"ec2:describeNatGateways",
"ec2:describeNetworkAcls",
"ec2:describeNetworkInterfaceAttribute",
"ec2:describeNetworkInterfaces",
"ec2:describePlacementGroups",
"ec2:describePrefixLists",
"ec2:describePrincipalIdFormat",
"ec2:describePublicIpv4Pools",
"ec2:describeRegions",
"ec2:describeReservedInstances",
"ec2:describeReservedInstancesListings",
"ec2:describeReservedInstancesModifications",
"ec2:describeReservedInstancesOfferings",
"ec2:describeRouteTables",
"ec2:describeScheduledInstanceAvailability",
"ec2:describeScheduledInstances",
"ec2:describeSecurityGroupReferences",
"ec2:describeSecurityGroupRules",
"ec2:describeSecurityGroups",
"ec2:describeSnapshotAttribute",
"ec2:describeSnapshots",
"ec2:describeSpotDatafeedSubscription",
"ec2:describeSpotFleetInstances",
"ec2:describeSpotFleetRequestHistory",
"ec2:describeSpotFleetRequests",
"ec2:describeSpotInstanceRequests",
"ec2:describeSpotPriceHistory",
```

```
"ec2:describeStaleSecurityGroups",
"ec2:describeStoreImageTasks",
"ec2:describeSubnets",
"ec2:describeTags",
"ec2:describeTrafficMirrorFilters",
"ec2:describeTrafficMirrorSessions",
"ec2:describeTrafficMirrorTargets",
"ec2:describeTransitGatewayAttachments",
"ec2:describeTransitGatewayConnectPeers",
"ec2:describeTransitGatewayMulticastDomains",
"ec2:describeTransitGatewayPeeringAttachments",
"ec2:describeTransitGatewayPolicyTables",
"ec2:describeTransitGatewayRouteTableAnnouncements",
"ec2:describeTransitGatewayRouteTables",
"ec2:describeTransitGateways",
"ec2:describeTransitGatewayVpcAttachments",
"ec2:describeVerifiedAccessEndpoints",
"ec2:describeVerifiedAccessGroups",
"ec2:describeVerifiedAccessInstances",
"ec2:describeVerifiedAccessTrustProviders",
"ec2:describeVolumeAttribute",
"ec2:describeVolumes",
"ec2:describeVolumesModifications",
"ec2:describeVolumeStatus",
"ec2:describeVpcAttribute",
"ec2:describeVpcClassicLink",
"ec2:describeVpcClassicLinkDnsSupport",
"ec2:describeVpcEndpointConnectionNotifications",
"ec2:describeVpcEndpointConnections",
"ec2:describeVpcEndpoints",
"ec2:describeVpcEndpointServiceConfigurations",
"ec2:describeVpcEndpointServicePermissions",
"ec2:describeVpcEndpointServices",
"ec2:describeVpcPeeringConnections",
"ec2:describeVpcs",
"ec2:describeVpnConnections",
"ec2:describeVpnGateways",
"ec2:getAssociatedIpv6PoolCidrs",
"ec2:getCapacityReservationUsage",
"ec2:getCoipPoolUsage",
"ec2:getConsoleOutput",
"ec2:getConsoleScreenshot",
"ec2:getDefaultCreditSpecification",
"ec2:getEbsDefaultKmsKeyId",
```

```
"ec2:getEbsEncryptionByDefault",
"ec2:getGroupsForCapacityReservation",
"ec2:getHostReservationPurchasePreview",
"ec2:getInstanceTypesFromInstanceRequirements",
"ec2:getIpamAddressHistory",
"ec2:getIpamPoolAllocations",
"ec2:getIpamPoolCidrs",
"ec2:getIpamResourceCidrs",
"ec2:getLaunchTemplateData",
"ec2:getManagedPrefixListAssociations",
"ec2:getManagedPrefixListEntries",
"ec2:getReservedInstancesExchangeQuote",
"ec2:getSerialConsoleAccessStatus",
"ec2:getSpotPlacementScores",
"ec2:getTransitGatewayMulticastDomainAssociations",
"ec2:getTransitGatewayPrefixListReferences",
"ec2:getVerifiedAccessEndpointPolicy",
"ec2:getVerifiedAccessGroupPolicy",
"ec2:listImagesInRecycleBin",
"ec2:listSnapshotsInRecycleBin",
"ec2:searchLocalGatewayRoutes",
"ec2:searchTransitGatewayMulticastGroups",
"ec2:searchTransitGatewayRoutes",
"ecr-public:describeImages",
"ecr-public:describeImageTags",
"ecr-public:describeRegistries",
"ecr-public:describeRepositories",
"ecr-public:getRegistryCatalogData",
"ecr-public:getRepositoryCatalogData",
"ecr-public:getRepositoryPolicy",
"ecr-public:listTagsForResource",
"ecr:batchCheckLayerAvailability",
"ecr:batchGetRepositoryScanningConfiguration",
"ecr:describeImages",
"ecr:describeImageReplicationStatus",
"ecr:describeImageScanFindings",
"ecr:describePullThroughCacheRules",
"ecr:describeRegistry",
"ecr:describeRepositories",
"ecr:getLifecyclePolicy",
"ecr:getLifecyclePolicyPreview",
"ecr:getRegistryPolicy",
"ecr:getRegistryScanningConfiguration",
"ecr:getRepositoryPolicy",
```

```
"ecr:listImages",
"ecr:listTagsForResource",
"ecs:describeCapacityProviders",
"ecs:describeClusters",
"ecs:describeContainerInstances",
"ecs:describeServices",
"ecs:describeTaskDefinition",
"ecs:describeTasks",
"ecs:describeTaskSets",
"ecs:getTaskProtection",
"ecs:listAccountSettings",
"ecs:listAttributes",
"ecs:listClusters",
"ecs:listContainerInstances",
"ecs:listServices",
"ecs:listServicesByNamespace",
"ecs:listTagsForResource",
"ecs:listTaskDefinitionFamilies",
"ecs:listTaskDefinitions",
"ecs:listTasks",
"eks:describeAccessEntry",
"eks:describeAddon",
"eks:describeAddonConfiguration",
"eks:describeAddonVersions",
"eks:describeCluster",
"eks:describeEksAnywhereSubscription",
"eks:describeFargateProfile",
"eks:describeIdentityProviderConfig",
"eks:describeNodegroup",
"eks:describeUpdate",
"eks:listAccessEntries",
"eks:listAccessPolicies",
"eks:listAddons",
"eks:listAssociatedAccessPolicies",
"eks:listClusters",
"eks:listEksAnywhereSubscriptions",
"eks:listFargateProfiles",
"eks:listIdentityProviderConfigs",
"eks:listNodegroups",
"eks:listUpdates",
"elasticache:describeCacheClusters",
"elasticache:describeCacheEngineVersions",
"elasticache:describeCacheParameterGroups",
"elasticache:describeCacheParameters",
```

```
"elasticache:describeCacheSecurityGroups",
"elasticache:describeCacheSubnetGroups",
"elasticache:describeEngineDefaultParameters",
"elasticache:describeEvents",
"elasticache:describeGlobalReplicationGroups",
"elasticache:describeReplicationGroups",
"elasticache:describeReservedCacheNodes",
"elasticache:describeReservedCacheNodesOfferings",
"elasticache:describeServerlessCaches",
"elasticache:describeServerlessCacheSnapshots",
"elasticache:describeServiceUpdates",
"elasticache:describeSnapshots",
"elasticache:describeUpdateActions",
"elasticache:describeUserGroups",
"elasticache:describeUsers",
"elasticache:listAllowedNodeTypeModifications",
"elasticache:listTagsForResource",
"elasticbeanstalk:checkDNSAvailability",
"elasticbeanstalk:describeAccountAttributes",
"elasticbeanstalk:describeApplicationVersions",
"elasticbeanstalk:describeApplications",
"elasticbeanstalk:describeConfigurationOptions",
"elasticbeanstalk:describeEnvironmentHealth",
"elasticbeanstalk:describeEnvironmentManagedActionHistory",
"elasticbeanstalk:describeEnvironmentManagedActions",
"elasticbeanstalk:describeEnvironmentResources",
"elasticbeanstalk:describeEnvironments",
"elasticbeanstalk:describeEvents",
"elasticbeanstalk:describeInstancesHealth",
"elasticbeanstalk:describePlatformVersion",
"elasticbeanstalk:listAvailableSolutionStacks",
"elasticbeanstalk:listPlatformBranches",
"elasticbeanstalk:listPlatformVersions",
"elasticbeanstalk:validateConfigurationSettings",
"elasticfilesystem:describeAccessPoints",
"elasticfilesystem:describeFileSystemPolicy",
"elasticfilesystem:describeFileSystems",
"elasticfilesystem:describeLifecycleConfiguration",
"elasticfilesystem:describeMountTargets",
"elasticfilesystem:describeMountTargetSecurityGroups",
"elasticfilesystem:describeTags",
"elasticfilesystem:listTagsForResource",
"elasticloadbalancing:describeAccountLimits",
"elasticloadbalancing:describeInstanceHealth",
```



```
"elasticloadbalancing:describeListenerCertificates",
"elasticloadbalancing:describeListeners",
"elasticloadbalancing:describeLoadBalancerAttributes",
"elasticloadbalancing:describeLoadBalancerPolicies",
"elasticloadbalancing:describeLoadBalancerPolicyTypes",
"elasticloadbalancing:describeLoadBalancers",
"elasticloadbalancing:describeRules",
"elasticloadbalancing:describeSSLPolicies",
"elasticloadbalancing:describeTags",
"elasticloadbalancing:describeTargetGroupAttributes",
"elasticloadbalancing:describeTargetGroups",
"elasticloadbalancing:describeTargetHealth",
"elasticmapreduce:describeCluster",
"elasticmapreduce:describeNotebookExecution",
"elasticmapreduce:describeReleaseLabel",
"elasticmapreduce:describeSecurityConfiguration",
"elasticmapreduce:describeStep",
"elasticmapreduce:describeStudio",
"elasticmapreduce:getAutoTerminationPolicy",
"elasticmapreduce:getBlockPublicAccessConfiguration",
"elasticmapreduce:getManagedScalingPolicy",
"elasticmapreduce:getStudioSessionMapping",
"elasticmapreduce:listBootstrapActions",
"elasticmapreduce:listClusters",
"elasticmapreduce:listInstanceFleets",
"elasticmapreduce:listInstanceGroups",
"elasticmapreduce:listInstances",
"elasticmapreduce:listNotebookExecutions",
"elasticmapreduce:listReleaseLabels",
"elasticmapreduce:listSecurityConfigurations",
"elasticmapreduce:listSteps",
"elasticmapreduce:listStudios",
"elasticmapreduce:listStudioSessionMappings",
"elastictranscoder:listJobsByPipeline",
"elastictranscoder:listJobsByStatus",
"elastictranscoder:listPipelines",
"elastictranscoder:listPresets",
"elastictranscoder:readPipeline",
"elastictranscoder:readPreset",
"emr-containers:describeJobRun",
"emr-containers:describeJobTemplate",
"emr-containers:describeManagedEndpoint",
"emr-containers:describeVirtualCluster",
"emr-containers:listJobRuns",
```

```
"emr-containers:listJobTemplates",
"emr-containers:listManagedEndpoints",
"emr-containers:listVirtualClusters",
"emr-serverless:getApplication",
"emr-serverless:getJobRun",
"emr-serverless:listApplications",
"es:describeDomain",
"es:describeDomainAutoTunes",
"es:describeDomainChangeProgress",
"es:describeDomainConfig",
"es:describeDomains",
"es:describeDryRunProgress",
"es:describeElasticsearchDomain",
"es:describeElasticsearchDomainConfig",
"es:describeElasticsearchDomains",
"es:describeInboundConnections",
"es:describeInstanceTypeLimits",
"es:describeOutboundConnections",
"es:describePackages",
"es:describeReservedInstanceOfferings",
"es:describeReservedInstances",
"es:describeVpcEndpoints",
"es:getCompatibleVersions",
"es:getPackageVersionHistory",
"es:getUpgradeHistory",
"es:getUpgradeStatus",
"es:listDomainNames",
"es:listDomainsForPackage",
"es:listInstanceTypeDetails",
"es:listPackagesForDomain",
"es:listScheduledActions",
"es:listTags",
"es:listVersions",
"es:listVpcEndpointAccess",
"es:listVpcEndpoints",
"es:listVpcEndpointsForDomain",
"evidently:getExperiment",
"evidently:getFeature",
"evidently:getLaunch",
"evidently:getProject",
"evidently:getSegment",
"evidently:listExperiments",
"evidently:listFeatures",
"evidently:listLaunches",
```

```
"evidently:listProjects",
"evidently:listSegments",
"evidently:listSegmentReferences",
"events:describeApiDestination",
"events:describeArchive",
"events:describeConnection",
"events:describeEndpoint",
"events:describeEventBus",
"events:describeEventSource",
"events:describePartnerEventSource",
"events:describeReplay",
"events:describeRule",
"events:listArchives",
"events:listApiDestinations",
"events:listConnections",
"events:listEndpoints",
"events:listEventBuses",
"events:listEventSources",
"events:listPartnerEventSourceAccounts",
"events:listPartnerEventSources",
"events:listReplays",
"events:listRuleNamesByTarget",
"events:listRules",
"events:listTargetsByRule",
"events:testEventPattern",
"firehose:describeDeliveryStream",
"firehose:listDeliveryStreams",
"fms:getAdminAccount",
"fms:getComplianceDetail",
"fms:getNotificationChannel",
"fms:getPolicy",
"fms:getProtectionStatus",
"fms:listComplianceStatus",
"fms:listMemberAccounts",
"fms:listPolicies",
"forecast:describeDataset",
"forecast:describeDatasetGroup",
"forecast:describeDatasetImportJob",
"forecast:describeForecast",
"forecast:describeForecastExportJob",
"forecast:describePredictor",
"forecast:getAccuracyMetrics",
"forecast:listDatasetGroups",
"forecast:listDatasetImportJobs",
```

```
"forecast:listDatasets",
"forecast:listForecastExportJobs",
"forecast:listForecasts",
"forecast:listPredictors",
"fsx:describeBackups",
"fsx:describeDataRepositoryAssociations",
"fsx:describeDataRepositoryTasks",
"fsx:describeFileCaches",
"fsx:describeFileSystems",
"fsx:describeSnapshots",
"fsx:describeStorageVirtualMachines",
"fsx:describeVolumes",
"fsx:listTagsForResource",
"gamelift:describeAlias",
"gamelift:describeBuild",
"gamelift:describeEC2InstanceLimits",
"gamelift:describeFleetAttributes",
"gamelift:describeFleetCapacity",
"gamelift:describeFleetEvents",
"gamelift:describeFleetLocationAttributes",
"gamelift:describeFleetLocationCapacity",
"gamelift:describeFleetLocationUtilization",
"gamelift:describeFleetPortSettings",
"gamelift:describeFleetUtilization",
"gamelift:describeGameServer",
"gamelift:describeGameServerGroup",
"gamelift:describeGameSessionDetails",
"gamelift:describeGameSessionPlacement",
"gamelift:describeGameSessionQueues",
"gamelift:describeGameSessions",
"gamelift:describeInstances",
"gamelift:describeMatchmaking",
"gamelift:describeMatchmakingConfigurations",
"gamelift:describeMatchmakingRuleSets",
"gamelift:describePlayerSessions",
"gamelift:describeRuntimeConfiguration",
"gamelift:describeScalingPolicies",
"gamelift:describeScript",
"gamelift:listAliases",
"gamelift:listBuilds",
"gamelift:listFleets",
"gamelift:listGameServerGroups",
"gamelift:listGameServers",
"gamelift:listScripts",
```

```
"gamelift:resolveAlias",
"glacier:describeJob",
"glacier:describeVault",
"glacier:getDataRetrievalPolicy",
"glacier:getVaultAccessPolicy",
"glacier:getVaultLock",
"glacier:getVaultNotifications",
"glacier:listJobs",
"glacier:listTagsForVault",
"glacier:listVaults",
"globalaccelerator:describeAccelerator",
"globalaccelerator:describeAcceleratorAttributes",
"globalaccelerator:describeEndpointGroup",
"globalaccelerator:describeListener",
"globalaccelerator:listAccelerators",
"globalaccelerator:listEndpointGroups",
"globalaccelerator:listListeners",
"glue:batchGetBlueprints",
"glue:batchGetCrawlers",
"glue:batchGetDevEndpoints",
"glue:batchGetJobs",
"glue:batchGetPartition",
"glue:batchGetTriggers",
"glue:batchGetWorkflows",
"glue:checkSchemaVersionValidity",
"glue:getBlueprint",
"glue:getBlueprintRun",
"glue:getBlueprintRuns",
"glue:getCatalogImportStatus",
"glue:getClassifier",
"glue:getClassifiers",
"glue:getColumnStatisticsForPartition",
"glue:getColumnStatisticsForTable",
"glue:getCrawler",
"glue:getCrawlerMetrics",
"glue:getCrawlers",
"glue:getCustomEntityType",
"glue:getDatabase",
"glue:getDatabases",
"glue:getDataflowGraph",
"glue:getDataQualityResult",
"glue:getDataQualityRuleRecommendationRun",
"glue:getDataQualityRuleset",
"glue:getDataQualityRulesetEvaluationRun",
```

```
"glue:getDevEndpoint",
"glue:getDevEndpoints",
"glue:getJob",
"glue:getJobRun",
"glue:getJobRuns",
"glue:getJobs",
"glue:getMapping",
"glue:getMLTaskRun",
"glue:getMLTaskRuns",
"glue:getMLTransform",
"glue:getMLTransforms",
"glue:getPartition",
"glue:getPartitionIndexes",
"glue:getPartitions",
"glue:getRegistry",
"glue:getResourcePolicies",
"glue:getResourcePolicy",
"glue:getSchema",
"glue:getSchemaByDefinition",
"glue:getSchemaVersion",
"glue:getSchemaVersionsDiff",
"glue:getSession",
"glue:getStatement",
"glue:getTable",
"glue:getTables",
"glue:getTableVersions",
"glue:getTrigger",
"glue:getTriggers",
"glue:getUserDefinedFunction",
"glue:getUserDefinedFunctions",
"glue:getWorkflow",
"glue:getWorkflowRun",
"glue:getWorkflowRuns",
"glue:listCrawlers",
"glue:listCrawls",
"glue:listDataQualityResults",
"glue:listDataQualityRuleRecommendationRuns",
"glue:listDataQualityRulesetEvaluationRuns",
"glue:listDataQualityRulesets",
"glue:listDevEndpoints",
"glue:listMLTransforms",
"glue:listRegistries",
"glue:listSchemas",
"glue:listSchemaVersions",
```

```
"glue:listSessions",
"glue:listStatements",
"glue:querySchemaVersionMetadata",
"grafana:describeWorkspace",
"grafana:describeWorkspaceAuthentication",
"grafana:listPermissions",
"grafana:listVersions",
"grafana:listWorkspaces",
"greengrass:getConnectivityInfo",
"greengrass:getCoreDefinition",
"greengrass:getCoreDefinitionVersion",
"greengrass:getDeploymentStatus",
"greengrass:getDeviceDefinition",
"greengrass:getDeviceDefinitionVersion",
"greengrass:getFunctionDefinition",
"greengrass:getFunctionDefinitionVersion",
"greengrass:getGroup",
"greengrass:getGroupCertificateAuthority",
"greengrass:getGroupVersion",
"greengrass:getLoggerDefinition",
"greengrass:getLoggerDefinitionVersion",
"greengrass:getResourceDefinitionVersion",
"greengrass:getServiceRoleForAccount",
"greengrass:getSubscriptionDefinition",
"greengrass:getSubscriptionDefinitionVersion",
"greengrass:listCoreDefinitions",
"greengrass:listCoreDefinitionVersions",
"greengrass:listDeployments",
"greengrass:listDeviceDefinitions",
"greengrass:listDeviceDefinitionVersions",
"greengrass:listFunctionDefinitions",
"greengrass:listFunctionDefinitionVersions",
"greengrass:listGroups",
"greengrass:listGroupVersions",
"greengrass:listLoggerDefinitions",
"greengrass:listLoggerDefinitionVersions",
"greengrass:listResourceDefinitions",
"greengrass:listResourceDefinitionVersions",
"greengrass:listSubscriptionDefinitions",
"greengrass:listSubscriptionDefinitionVersions",
"guardduty:getDetector",
"guardduty:getFindings",
"guardduty:getFindingsStatistics",
"guardduty:getInvitationsCount",
```

```
"guardduty:getIPSet",
"guardduty:getMasterAccount",
"guardduty:getMembers",
"guardduty:getThreatIntelSet",
"guardduty:listDetectors",
"guardduty:listFindings",
"guardduty:listInvitations",
"guardduty:listIPSets",
"guardduty:listMembers",
"guardduty:listThreatIntelSets",
"health:describeAffectedAccountsForOrganization",
"health:describeAffectedEntities",
"health:describeAffectedEntitiesForOrganization",
"health:describeEntityAggregates",
"health:describeEntityAggregatesForOrganization",
"health:describeEventAggregates",
"health:describeEventDetails",
"health:describeEventDetailsForOrganization",
"health:describeEvents",
"health:describeEventsForOrganization",
"health:describeEventTypes",
"health:describeHealthServiceStatusForOrganization",
"iam:getAccessKeyLastUsed",
"iam:getAccountAuthorizationDetails",
"iam:getAccountPasswordPolicy",
"iam:getAccountSummary",
"iam:getContextKeysForCustomPolicy",
"iam:getContextKeysForPrincipalPolicy",
"iam:getCredentialReport",
"iam:getGroup",
"iam:getGroupPolicy",
"iam:getInstanceProfile",
"iam:getLoginProfile",
"iam:getOpenIDConnectProvider",
"iam:getPolicy",
"iam:getPolicyVersion",
"iam:getRole",
"iam:getRolePolicy",
"iam:getSAMLProvider",
"iam:getServerCertificate",
"iam:getServiceLinkedRoleDeletionStatus",
"iam:getSSHPublicKey",
"iam:getUser",
"iam:getUserPolicy",
```



```
"iam:listAccessKeys",
"iam:listAccountAliases",
"iam:listAttachedGroupPolicies",
"iam:listAttachedRolePolicies",
"iam:listAttachedUserPolicies",
"iam:listEntitiesForPolicy",
"iam:listGroupPolicies",
"iam:listGroups",
"iam:listGroupsForUser",
"iam:listInstanceProfiles",
"iam:listInstanceProfilesForRole",
"iam:listMFADevices",
"iam:listOpenIDConnectProviders",
"iam:listPolicies",
"iam:listPolicyVersions",
"iam:listRolePolicies",
"iam:listRoles",
"iam:listSAMLProviders",
"iam:listServerCertificates",
"iam:listSigningCertificates",
"iam:listSSHPublicKeys",
"iam:listUserPolicies",
"iam:listUsers",
"iam:listVirtualMFADevices",
"iam:simulateCustomPolicy",
"iam:simulatePrincipalPolicy",
"imagebuilder:getComponent",
"imagebuilder:getComponentPolicy",
"imagebuilder:getContainerRecipe",
"imagebuilder:getDistributionConfiguration",
"imagebuilder:getImage",
"imagebuilder:getImagePipeline",
"imagebuilder:getImagePolicy",
"imagebuilder:getImageRecipe",
"imagebuilder:getImageRecipePolicy",
"imagebuilder:getInfrastructureConfiguration",
"imagebuilder:getLifecycleExecution",
"imagebuilder:getLifecyclePolicy",
"imagebuilder:getWorkflow",
"imagebuilder:getWorkflowExecution",
"imagebuilder:getWorkflowStepExecution",
"imagebuilder:listComponentBuildVersions",
"imagebuilder:listComponents",
"imagebuilder:listContainerRecipes",
```

```
"imagebuilder:listDistributionConfigurations",
"imagebuilder:listImageBuildVersions",
"imagebuilder:listImagePipelineImages",
"imagebuilder:listImagePipelines",
"imagebuilder:listImageRecipes",
"imagebuilder:listImages",
"imagebuilder:listImageScanFindingAggregations",
"imagebuilder:listInfrastructureConfigurations",
"imagebuilder:listLifecycleExecutions",
"imagebuilder:listLifecycleExecutionResources",
"imagebuilder:listLifecyclePolicies",
"imagebuilder:listWorkflowBuildVersions",
"imagebuilder:listWorkflowExecutions",
"imagebuilder:listWorkflows",
"imagebuilder:listWorkflowStepExecutions",
"imagebuilder:listTagsForResource",
"inspector:describeAssessmentRuns",
"inspector:describeAssessmentTargets",
"inspector:describeAssessmentTemplates",
"inspector:describeCrossAccountAccessRole",
"inspector:describeResourceGroups",
"inspector:describeRulesPackages",
"inspector:getTelemetryMetadata",
"inspector:listAssessmentRunAgents",
"inspector:listAssessmentRuns",
"inspector:listAssessmentTargets",
"inspector:listAssessmentTemplates",
"inspector:listEventSubscriptions",
"inspector:listRulesPackages",
"inspector:listTagsForResource",
"inspector2:batchGetAccountStatus",
"inspector2:batchGetFreeTrialInfo",
"inspector2:describeOrganizationConfiguration",
"inspector2:getDelegatedAdminAccount",
"inspector2:getMember",
"inspector2:getSbomExport",
"inspector2:listCisScanConfigurations",
"inspector2:listCisScanResultsAggregatedByChecks",
"inspector2:listCisScanResultsAggregatedByTargetResource",
"inspector2:listCisScans",
"inspector2:listCoverage",
"inspector2:listDelegatedAdminAccounts",
"inspector2:listFilters",
"inspector2:listFindings",
```

```
"inspector2:listMembers",
"inspector2:listUsageTotals",
"inspector-scan:scanSbom",
"internetmonitor:getMonitor",
"internetmonitor:listMonitors",
"internetmonitor:getHealthEvent",
"internetmonitor:listHealthEvents",
"iot:describeAuthorizer",
"iot:describeCACertificate",
"iot:describeCertificate",
"iot:describeDefaultAuthorizer",
"iot:describeDomainConfiguration",
"iot:describeEndpoint",
"iot:describeIndex",
"iot:describeJobExecution",
"iot:describeThing",
"iot:describeThingGroup",
"iot:describeTunnel",
"iot:getEffectivePolicies",
"iot:getIndexingConfiguration",
"iot:getLoggingOptions",
"iot:getPolicy",
"iot:getPolicyVersion",
"iot:getTopicRule",
"iot:getV2LoggingOptions",
"iot:listAttachedPolicies",
"iot:listAuthorizers",
"iot:listCACertificates",
"iot:listCertificates",
"iot:listCertificatesByCA",
"iot:listDomainConfigurations",
"iot:listJobExecutionsForJob",
"iot:listJobExecutionsForThing",
"iot:listJobs",
"iot:listNamedShadowsForThing",
"iot:listOutgoingCertificates",
"iot:listPackages",
"iot:listPackageVersions",
"iot:listPolicies",
"iot:listPolicyPrincipals",
"iot:listPolicyVersions",
"iot:listPrincipalPolicies",
"iot:listPrincipalThings",
"iot:listRoleAliases",
```

```
"iot:listTargetsForPolicy",
"iot:listThingGroups",
"iot:listThingGroupsForThing",
"iot:listThingPrincipals",
"iot:listThingRegistrationTasks",
"iot:listThings",
"iot:listThingsInThingGroup",
"iot:listThingTypes",
"iot:listTopicRules",
"iot:listTunnels",
"iot:listV2LoggingLevels",
"iotevents:describeDetector",
"iotevents:describeDetectorModel",
"iotevents:describeInput",
"iotevents:describeLoggingOptions",
"iotevents:listDetectorModels",
"iotevents:listDetectorModelVersions",
"iotevents:listDetectors",
"iotevents:listInputs",
"iotfleetwise:getCampaign",
"iotfleetwise:getDecoderManifest",
"iotfleetwise:getFleet",
"iotfleetwise:getModelManifest",
"iotfleetwise:getSignalCatalog",
"iotfleetwise:getVehicle",
"iotfleetwise:getVehicleStatus",
"iotfleetwise:listCampaigns",
"iotfleetwise:listDecoderManifests",
"iotfleetwise:listDecoderManifestNetworkInterfaces",
"iotfleetwise:listDecoderManifestSignals",
"iotfleetwise:listFleets",
"iotfleetwise:listFleetsForVehicle",
"iotfleetwise:listModelManifests",
"iotfleetwise:listModelManifestNodes",
"iotfleetwise:listSignalCatalogs",
"iotfleetwise:listSignalCatalogNodes",
"iotfleetwise:listVehicles",
"iotsitewise:describeAccessPolicy",
"iotsitewise:describeAsset",
"iotsitewise:describeAssetModel",
"iotsitewise:describeAssetProperty",
"iotsitewise:describeDashboard",
"iotsitewise:describeGateway",
"iotsitewise:describeGatewayCapabilityConfiguration",
```

```
"iotsitewise:describeLoggingOptions",
"iotsitewise:describePortal",
"iotsitewise:describeProject",
"iotsitewise:listAccessPolicies",
"iotsitewise:listAssetModels",
"iotsitewise:listAssets",
"iotsitewise:listAssociatedAssets",
"iotsitewise:listDashboards",
"iotsitewise:listGateways",
"iotsitewise:listPortals",
"iotsitewise:listProjectAssets",
"iotsitewise:listProjects",
"iottwinmaker:getComponentType",
"iottwinmaker:getEntity",
"iottwinmaker:getPricingPlan",
"iottwinmaker:getScene",
"iottwinmaker:getWorkspace",
"iottwinmaker:listComponentTypes",
"iottwinmaker:listEntities",
"iottwinmaker:listScenes",
"iottwinmaker:getSyncJob",
"iottwinmaker:listSyncJobs",
"iottwinmaker:listSyncResources",
"iottwinmaker:listWorkspaces",
"iotwireless:getDestination",
"iotwireless:getDeviceProfile",
"iotwireless:getPartnerAccount",
"iotwireless:getServiceEndpoint",
"iotwireless:getServiceProfile",
"iotwireless:getWirelessDevice",
"iotwireless:getWirelessDeviceStatistics",
"iotwireless:getWirelessGateway",
"iotwireless:getWirelessGatewayCertificate",
"iotwireless:getWirelessGatewayFirmwareInformation",
"iotwireless:getWirelessGatewayStatistics",
"iotwireless:getWirelessGatewayTask",
"iotwireless:getWirelessGatewayTaskDefinition",
"iotwireless:listDestinations",
"iotwireless:listDeviceProfiles",
"iotwireless:listPartnerAccounts",
"iotwireless:listServiceProfiles",
"iotwireless:listTagsForResource",
"iotwireless:listWirelessDevices",
"iotwireless:listWirelessGateways",
```

```
"iotwireless:listWirelessGatewayTaskDefinitions",
"ivs:getChannel",
"ivs:getRecordingConfiguration",
"ivs:getStream",
"ivs:getStreamSession",
"ivs:listChannels",
"ivs:listPlaybackKeyPairs",
"ivs:listRecordingConfigurations",
"ivs:listStreamKeys",
"ivs:listStreams",
"ivs:listStreamSessions",
"kafka:describeCluster",
"kafka:describeClusterOperation",
"kafka:describeClusterOperationV2",
"kafka:describeClusterV2",
"kafka:describeConfiguration",
"kafka:describeConfigurationRevision",
"kafka:describeReplicator",
"kafka:describeVpcConnection",
"kafka:getBootstrapBrokers",
"kafka:getClusterPolicy",
"kafka:listConfigurations",
"kafka:listConfigurationRevisions",
"kafka:listClientVpcConnections",
"kafka:listClusterOperations",
"kafka:listClusterOperationsV2",
"kafka:listClusters",
"kafka:listClustersV2",
"kafka:listNodes",
"kafka:listReplicators",
"kafka:listScramSecrets",
"kafka:listVpcConnections",
"kafkaconnect:describeConnector",
"kafkaconnect:describeCustomPlugin",
"kafkaconnect:describeWorkerConfiguration",
"kafkaconnect:listConnectors",
"kafkaconnect:listCustomPlugins",
"kafkaconnect:listWorkerConfigurations",
"kendra:describeDataSource",
"kendra:describeFaq",
"kendra:describeIndex",
"kendra:listDataSources",
"kendra:listFaqs",
"kendra:listIndices",
```

```
"kinesis:describeStream",
"kinesis:describeStreamConsumer",
"kinesis:describeStreamSummary",
"kinesis:listShards",
"kinesis:listStreams",
"kinesis:listStreamConsumers",
"kinesis:listTagsForStream",
"kinesisanalytics:describeApplication",
"kinesisanalytics:describeApplicationSnapshot",
"kinesisanalytics:listApplications",
"kinesisanalytics:listApplicationSnapshots",
"kinesisvideo:describeImageGenerationConfiguration",
"kinesisvideo:describeNotificationConfiguration",
"kinesisvideo:describeSignalingChannel",
"kinesisvideo:describeStream",
"kinesisvideo:getDataEndpoint",
"kinesisvideo:getIceServerConfig",
"kinesisvideo:getSignalingChannelEndpoint",
"kinesisvideo:listSignalingChannels",
"kinesisvideo:listStreams",
"kms:describeKey",
"kms:getKeyPolicy",
"kms:getKeyRotationStatus",
"kms:listAliases",
"kms:listGrants",
"kms:listKeyPolicies",
"kms:listKeys",
"kms:listResourceTags",
"kms:listRetirableGrants",
"lambda:getAccountSettings",
"lambda:getAlias",
"lambda:getCodeSigningConfig",
"lambda:getEventSourceMapping",
"lambda:getFunction",
"lambda:getFunctionCodeSigningConfig",
"lambda:getFunctionConcurrency",
"lambda:getFunctionConfiguration",
"lambda:getFunctionEventInvokeConfig",
"lambda:getFunctionUrlConfig",
"lambda:getLayerVersion",
"lambda:getLayerVersionPolicy",
"lambda:getPolicy",
"lambda:getProvisionedConcurrencyConfig",
"lambda:getRuntimeManagementConfig",
```

```
"lambda:listAliases",
"lambda:listCodeSigningConfigs",
"lambda:listEventSourceMappings",
"lambda:listFunctionEventInvokeConfigs",
"lambda:listFunctions",
"lambda:listFunctionsByCodeSigningConfig",
"lambda:listFunctionUrlConfigs",
"lambda:listLayers",
"lambda:listLayerVersions",
"lambda:listProvisionedConcurrencyConfigs",
"lambda:listVersionsByFunction",
"launchwizard:describeProvisionedApp",
"launchwizard:describeProvisioningEvents",
"launchwizard:listProvisionedApps",
"lex:describeBot",
"lex:describeBotAlias",
"lex:describeBotLocale",
"lex:describeBotRecommendation",
"lex:describeBotVersion",
"lex:describeCustomVocabularyMetadata",
"lex:describeExport",
"lex:describeImport",
"lex:describeIntent",
"lex:describeResourcePolicy",
"lex:describeSlot",
"lex:describeSlotType",
"lex:getBot",
"lex:getBotAlias",
"lex:getBotAliases",
"lex:getBotChannelAssociation",
"lex:getBotChannelAssociations",
"lex:getBots",
"lex:getBotVersions",
"lex:getBuiltinIntent",
"lex:getBuiltinIntents",
"lex:getBuiltinSlotTypes",
"lex:getIntent",
"lex:getIntents",
"lex:getIntentVersions",
"lex:getSlotType",
"lex:getSlotTypes",
"lex:getSlotTypeVersions",
"lex:listBotAliases",
"lex:listBotLocales",
```



```
"lex:listBotRecommendations",
"lex:listBots",
"lex:listBotVersions",
"lex:listExports",
"lex:listImports",
"lex:listIntents",
"lex:listRecommendedIntents",
"lex:listSlots",
"lex:listSlotTypes",
"license-manager:getLicenseConfiguration",
"license-manager:getServiceSettings",
"license-manager:listAssociationsForLicenseConfiguration",
"license-manager:listFailuresForLicenseConfigurationOperations",
"license-manager:listLicenseConfigurations",
"license-manager:listLicenseSpecificationsForResource",
"license-manager:listResourceInventory",
"license-manager:listUsageForLicenseConfiguration",
"lightsail:getActiveNames",
"lightsail:getAlarms",
"lightsail:getAutoSnapshots",
"lightsail:getBlueprints",
"lightsail:getBucketBundles",
"lightsail:getBucketMetricData",
"lightsail:getBuckets",
"lightsail:getBundles",
"lightsail:getCertificates",
"lightsail:getContainerImages",
"lightsail:getContainerServiceDeployments",
"lightsail:getContainerServiceMetricData",
"lightsail:getContainerServicePowers",
"lightsail:getContainerServices",
"lightsail:getDisk",
"lightsail:getDisks",
"lightsail:getDiskSnapshot",
"lightsail:getDiskSnapshots",
"lightsail:getDistributionBundles",
"lightsail:getDistributionMetricData",
"lightsail:getDistributions",
"lightsail:getDomain",
"lightsail:getDomains",
"lightsail:getExportSnapshotRecords",
"lightsail:getInstance",
"lightsail:getInstanceMetricData",
"lightsail:getInstancePortStates",
```

```
"lightsail:getInstances",
"lightsail:getInstanceSnapshot",
"lightsail:getInstanceSnapshots",
"lightsail:getInstanceState",
"lightsail:getKeyPair",
"lightsail:getKeyPairs",
"lightsail:getLoadBalancer",
"lightsail:getLoadBalancerMetricData",
"lightsail:getLoadBalancers",
"lightsail:getLoadBalancerTlsCertificates",
"lightsail:getOperation",
"lightsail:getOperations",
"lightsail:getOperationsForResource",
"lightsail:getRegions",
"lightsail:getRelationalDatabase",
"lightsail:getRelationalDatabaseMetricData",
"lightsail:getRelationalDatabases",
"lightsail:getRelationalDatabaseSnapshot",
"lightsail:getRelationalDatabaseSnapshots",
"lightsail:getStaticIp",
"lightsail:getStaticIps",
"lightsail:isVpcPeered",
"logs:describeAccountPolicies",
"logs:describeDeliveries",
"logs:describeDeliveryDestinations",
"logs:describeDeliverySources",
"logs:describeDestinations",
"logs:describeExportTasks",
"logs:describeLogGroups",
"logs:describeLogStreams",
"logs:describeMetricFilters",
"logs:describeQueries",
"logs:describeQueryDefinitions",
"logs:describeResourcePolicies",
"logs:describeSubscriptionFilters",
"logs:getDataProtectionPolicy",
"logs:getDelivery",
"logs:getDeliveryDestination",
"logs:getDeliveryDestinationPolicy",
"logs:getDeliverySource",
"logs:getLogAnomalyDetector",
"logs:getLogDelivery",
"logs:getLogGroupFields",
"logs:listAnomalies",
```

```
"logs:listLogAnomalyDetectors",
"logs:listLogDeliveries",
"logs:testMetricFilter",
"lookoutequipment:describeDataIngestionJob",
"lookoutequipment:describeDataset",
"lookoutequipment:describeInferenceScheduler",
"lookoutequipment:describeModel",
"lookoutequipment:listDataIngestionJobs",
"lookoutequipment:listDatasets",
"lookoutequipment:listInferenceExecutions",
"lookoutequipment:listInferenceSchedulers",
"lookoutequipment:listModels",
"lookoutmetrics:describeAlert",
"lookoutmetrics:describeAnomalyDetectionExecutions",
"lookoutmetrics:describeAnomalyDetector",
"lookoutmetrics:describeMetricSet",
"lookoutmetrics:getAnomalyGroup",
"lookoutmetrics:getDataQualityMetrics",
"lookoutmetrics:getFeedback",
"lookoutmetrics:getSampleData",
"lookoutmetrics:listAlerts",
"lookoutmetrics:listAnomalyDetectors",
"lookoutmetrics:listAnomalyGroupSummaries",
"lookoutmetrics:listAnomalyGroupTimeSeries",
"lookoutmetrics:listMetricSets",
"lookoutmetrics:listTagsForResource",
"machinelearning:describeBatchPredictions",
"machinelearning:describeDataSources",
"machinelearning:describeEvaluations",
"machinelearning:describeMLModels",
"machinelearning:getBatchPrediction",
"machinelearning:getDataSource",
"machinelearning:getEvaluation",
"machinelearning:getMLModel",
"macie2:getClassificationExportConfiguration",
"macie2:getCustomDataIdentifier",
"macie2:getFindings",
"macie2:getFindingStatistics",
"macie2:listClassificationJobs",
"macie2:listCustomDataIdentifiers",
"macie2:listFindings",
"managedblockchain:getMember",
"managedblockchain:getNetwork",
"managedblockchain:getNode",
```

```
"managedblockchain:listMembers",
"managedblockchain:listNetworks",
"managedblockchain:listNodes",
"mediaconnect:describeFlow",
"mediaconnect:listEntitlements",
"mediaconnect:listFlows",
"mediaconvert:describeEndpoints",
"mediaconvert:getJob",
"mediaconvert:getJobTemplate",
"mediaconvert:getPreset",
"mediaconvert:getQueue",
"mediaconvert:listJobs",
"mediaconvert:listJobTemplates",
"medialive:describeChannel",
"medialive:describeInput",
"medialive:describeInputDevice",
"medialive:describeInputSecurityGroup",
"medialive:describeMultiplex",
"medialive:describeOffering",
"medialive:describeReservation",
"medialive:describeSchedule",
"medialive:listChannels",
"medialive:listInputDevices",
"medialive:listInputs",
"medialive:listInputSecurityGroups",
"medialive:listMultiplexes",
"medialive:listOfferings",
"medialive:listReservations",
"mediapackage:describeChannel",
"mediapackage:describeOriginEndpoint",
"mediapackage:listChannels",
"mediapackage:listOriginEndpoints",
"mediastore:describeContainer",
"mediastore:getContainerPolicy",
"mediastore:getCorsPolicy",
"mediastore:listContainers",
"mediatailor:getPlaybackConfiguration",
"mediatailor:listPlaybackConfigurations",
"medical-imaging:getDatastore",
"medical-imaging:listDatastores",
"mgn:describeJobLogItems",
"mgn:describeJobs",
"mgn:describeLaunchConfigurationTemplates",
"mgn:describeReplicationConfigurationTemplates",
```

```
"mgn:describeSourceServers",
"mgn:describeVcenterClients",
"mgn:getLaunchConfiguration",
"mgn:getReplicationConfiguration",
"mgn:listApplications",
"mgn:listSourceServerActions",
"mgn:listTemplateActions",
"mgn:listWaves",
"mobiletargeting:getAdmChannel",
"mobiletargeting:getApnsChannel",
"mobiletargeting:getApnsSandboxChannel",
"mobiletargeting:getApnsVoipChannel",
"mobiletargeting:getApnsVoipSandboxChannel",
"mobiletargeting:getApp",
"mobiletargeting:getApplicationSettings",
"mobiletargeting:getApps",
"mobiletargeting:getBaiduChannel",
"mobiletargeting:getCampaign",
"mobiletargeting:getCampaignActivities",
"mobiletargeting:getCampaigns",
"mobiletargeting:getCampaignVersion",
"mobiletargeting:getCampaignVersions",
"mobiletargeting:getEmailChannel",
"mobiletargeting:getEndpoint",
"mobiletargeting:getEventStream",
"mobiletargeting:getExportJob",
"mobiletargeting:getExportJobs",
"mobiletargeting:getGcmChannel",
"mobiletargeting:getImportJob",
"mobiletargeting:getImportJobs",
"mobiletargeting:getJourney",
"mobiletargeting:getJourneyExecutionMetrics",
"mobiletargeting:getJourneyExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionActivityMetrics",
"mobiletargeting:getJourneyRunExecutionMetrics",
"mobiletargeting:getJourneyRuns",
"mobiletargeting:getSegment",
"mobiletargeting:getSegmentImportJobs",
"mobiletargeting:getSegments",
"mobiletargeting:getSegmentVersion",
"mobiletargeting:getSegmentVersions",
"mobiletargeting:getSmsChannel",
"mobiletargeting:listJourneys",
"mq:describeBroker",
```

```
"mq:describeConfiguration",
"mq:describeConfigurationRevision",
"mq:describeUser",
"mq:listBrokers",
"mq:listConfigurationRevisions",
"mq:listConfigurations",
"mq:listUsers",
"m2:getApplication",
"m2:getApplicationVersion",
"m2:getBatchJobExecution",
"m2:getDataSetDetails",
"m2:getDataSetImportTask",
"m2:getDeployment",
"m2:getEnvironment",
"m2:listApplications",
"m2:listApplicationVersions",
"m2:listBatchJobDefinitions",
"m2:listBatchJobExecutions",
"m2:listDataSetImportHistory",
"m2:listDataSets",
"m2:listDeployments",
"m2:listEngineVersions",
"m2:listEnvironments",
"network-firewall:describeFirewall",
"network-firewall:describeFirewallPolicy",
"network-firewall:describeLoggingConfiguration",
"network-firewall:describeRuleGroup",
"network-firewall:describeTlsInspectionConfiguration",
"network-firewall:listFirewallPolicies",
"network-firewall:listFirewalls",
"network-firewall:listRuleGroups",
"network-firewall:listTlsInspectionConfigurations",
"networkmanager:describeGlobalNetworks",
"networkmanager:getConnectAttachment",
"networkmanager:getConnections",
"networkmanager:getConnectPeer",
"networkmanager:getConnectPeerAssociations",
"networkmanager:getCoreNetwork",
"networkmanager:getCoreNetworkChangeEvents",
"networkmanager:getCoreNetworkChangeSet",
"networkmanager:getCoreNetworkPolicy",
"networkmanager:getCustomerGatewayAssociations",
"networkmanager:getDevices",
"networkmanager:getLinkAssociations",
```

```
"networkmanager:getLinks",
"networkmanager:getNetworkResourceCounts",
"networkmanager:getNetworkResourceRelationships",
"networkmanager:getNetworkResources",
"networkmanager:getNetworkRoutes",
"networkmanager:getNetworkTelemetry",
"networkmanager:getResourcePolicy",
"networkmanager:getRouteAnalysis",
"networkmanager:getSites",
"networkmanager:getSiteToSiteVpnAttachment",
"networkmanager:getTransitGatewayConnectPeerAssociations",
"networkmanager:getTransitGatewayPeering",
"networkmanager:getTransitGatewayRegistrations",
"networkmanager:getTransitGatewayRouteTableAttachment",
"networkmanager:getVpcAttachment",
"networkmanager:listAttachments",
"networkmanager:listConnectPeers",
"networkmanager:listCoreNetworkPolicyVersions",
"networkmanager:listCoreNetworks",
"networkmanager:listOrganizationServiceAccessStatus",
"networkmanager:listPeerings",
"networkmanager:listTagsForResource",
"networkmonitor:getMonitor",
"networkmonitor:getProbe",
"networkmonitor:listMonitors",
"nimble:getEula",
"nimble:getLaunchProfile",
"nimble:getLaunchProfileDetails",
"nimble:getLaunchProfileInitialization",
"nimble:getLaunchProfileMember",
"nimble:getStreamingImage",
"nimble:getStreamingSession",
"nimble:getStreamingSessionStream",
"nimble:getStudio",
"nimble:getStudioComponent",
"nimble:listEulaAcceptances",
"nimble:listEulas",
"nimble:listLaunchProfiles",
"nimble:listStreamingImages",
"nimble:listStreamingSessions",
"nimble:listStudioComponents",
"nimble:listStudios",
"notifications:getEventRule",
"notifications:getNotificationConfiguration",
```

```
"notifications:getNotificationEvent",
"notifications:listChannels",
"notifications:listEventRules",
"notifications:listNotificationConfigurations",
"notifications:listNotificationEvents",
"notifications:listNotificationHubs",
"notifications-contacts:getEmailContact",
"notifications-contacts:listEmailContacts",
"oam:getLink",
"oam:getSink",
"oam:getSinkPolicy",
"oam:listAttachedLinks",
"oam:listLinks",
"oam:listSinks",
"omics:getAnnotationImportJob",
"omics:getAnnotationStore",
"omics:getReadSetImportJob",
"omics:getReadSetMetadata",
"omics:getReference",
"omics:getReferenceImportJob",
"omics:getReferenceMetadata",
"omics:getReferenceStore",
"omics:getRun",
"omics:getRunGroup",
"omics:getSequenceStore",
"omics:getVariantImportJob",
"omics:getVariantStore",
"omics:getWorkflow",
"omics:listAnnotationImportJobs",
"omics:listAnnotationStores",
"omics:listMultipartReadSetUploads",
"omics:listReadSetImportJobs",
"omics:listReadSets",
"omics:listReadSetUploadParts",
"omics:listReferenceImportJobs",
"omics:listReferenceStores",
"omics:listReferences",
"omics:listRunGroups",
"omics:listRunTasks",
"omics:listRuns",
"omics:listSequenceStores",
"omics:listVariantImportJobs",
"omics:listVariantStores",
"omics:listWorkflows",
```



```
"opsworks-cm:describeAccountAttributes",
"opsworks-cm:describeBackups",
"opsworks-cm:describeEvents",
"opsworks-cm:describeNodeAssociationStatus",
"opsworks-cm:describeServers",
"opsworks:describeAgentVersions",
"opsworks:describeApps",
"opsworks:describeCommands",
"opsworks:describeDeployments",
"opsworks:describeEcsClusters",
"opsworks:describeElasticIps",
"opsworks:describeElasticLoadBalancers",
"opsworks:describeInstances",
"opsworks:describeLayers",
"opsworks:describeLoadBasedAutoScaling",
"opsworks:describeMyUserProfile",
"opsworks:describePermissions",
"opsworks:describeRaidArrays",
"opsworks:describeRdsDbInstances",
"opsworks:describeServiceErrors",
"opsworks:describeStackProvisioningParameters",
"opsworks:describeStacks",
"opsworks:describeStackSummary",
"opsworks:describeTimeBasedAutoScaling",
"opsworks:describeUserProfiles",
"opsworks:describeVolumes",
"opsworks:getHostnameSuggestion",
"organizations:listAccounts",
"organizations:listTagsForResource",
"outposts:getCatalogItem",
"outposts:getConnection",
"outposts:getOrder",
"outposts:getOutpost",
"outposts:getOutpostInstanceTypes",
"outposts:getSite",
"outposts:listAssets",
"outposts:listCatalogItems",
"outposts:listOrders",
"outposts:listOutposts",
"outposts:listSites",
"personalize:describeAlgorithm",
"personalize:describeBatchInferenceJob",
"personalize:describeBatchSegmentJob",
"personalize:describeCampaign",
```

```
"personalize:describeDataset",
"personalize:describeDatasetExportJob",
"personalize:describeDatasetGroup",
"personalize:describeDatasetImportJob",
"personalize:describeEventTracker",
"personalize:describeFeatureTransformation",
"personalize:describeFilter",
"personalize:describeRecipe",
"personalize:describeRecommender",
"personalize:describeSchema",
"personalize:describeSolution",
"personalize:describeSolutionVersion",
"personalize:getPersonalizedRanking",
"personalize:getRecommendations",
"personalize:getSolutionMetrics",
"personalize:listBatchInferenceJobs",
"personalize:listBatchSegmentJobs",
"personalize:listCampaigns",
"personalize:listDatasetExportJobs",
"personalize:listDatasetGroups",
"personalize:listDatasetImportJobs",
"personalize:listDatasets",
"personalize:listEventTrackers",
"personalize:listRecipes",
"personalize:listRecommenders",
"personalize:listSchemas",
"personalize:listSolutions",
"personalize:listSolutionVersions",
"pipes:describePipe",
"pipes:listPipes",
"pipes:listTagsForResource",
"polly:describeVoices",
"polly:getLexicon",
"polly:listLexicons",
"pricing:describeServices",
"pricing:getAttributeValues",
"pricing:getProducts",
"private-networks:getDeviceIdentifier",
"private-networks:getNetwork",
"private-networks:getNetworkResource",
"private-networks:listDeviceIdentifiers",
"private-networks:listNetworks",
"private-networks:listNetworkResources",
"qbusiness:getApplication",
```

```
"qbusiness:getDataSource",
"qbusiness:getIndex",
"qbusiness:getRetriever",
"qbusiness:getWebExperience",
"qbusiness:listApplications",
"qbusiness:listDataSources",
"qbusiness:listDataSourceSyncJobs",
"qbusiness:listIndices",
"qbusiness:listRetrievers",
"qbusiness:listWebExperiences",
"quicksight:describeAccountCustomization",
"quicksight:describeAccountSettings",
"quicksight:describeAccountSubscription",
"quicksight:describeAnalysis",
"quicksight:describeAnalysisPermissions",
"quicksight:describeDashboard",
"quicksight:describeDashboardPermissions",
"quicksight:describeDataSet",
"quicksight:describeDataSetPermissions",
"quicksight:describeDataSetRefreshProperties",
"quicksight:describeDataSource",
"quicksight:describeDataSourcePermissions",
"quicksight:describeFolder",
"quicksight:describeFolderPermissions",
"quicksight:describeFolderResolvedPermissions",
"quicksight:describeGroup",
"quicksight:describeGroupMembership",
"quicksight:describeIAMPolicyAssignment",
"quicksight:describeIngestion",
"quicksight:describeIpRestriction",
"quicksight:describeNamespace",
"quicksight:describeRefreshSchedule",
"quicksight:describeTemplate",
"quicksight:describeTemplateAlias",
"quicksight:describeTemplatePermissions",
"quicksight:describeTheme",
"quicksight:describeThemeAlias",
"quicksight:describeThemePermissions",
"quicksight:describeTopic",
"quicksight:describeTopicPermissions",
"quicksight:describeTopicRefresh",
"quicksight:describeTopicRefreshSchedule",
"quicksight:describeUser",
"quicksight:describeVPCCConnection",
```

```
"quicksight:listAnalyses",
"quicksight:listDashboards",
"quicksight:listDashboardVersions",
"quicksight:listDataSets",
"quicksight:listDataSources",
"quicksight:listFolderMembers",
"quicksight:listFolders",
"quicksight:listGroupMemberships",
"quicksight:listGroups",
"quicksight:listIAMPolicyAssignments",
"quicksight:listIAMPolicyAssignmentsForUser",
"quicksight:listIngestions",
"quicksight:listNamespaces",
"quicksight:listRefreshSchedules",
"quicksight:listTemplateAliases",
"quicksight:listTemplates",
"quicksight:listTemplateVersions",
"quicksight:listThemeAliases",
"quicksight:listThemes",
"quicksight:listThemeVersions",
"quicksight:listTopicRefreshSchedules",
"quicksight:listTopics",
"quicksight:listUserGroups",
"quicksight:listUsers",
"quicksight:listVPCConnections",
"quicksight:searchAnalyses",
"quicksight:searchDashboards",
"quicksight:searchDataSets",
"quicksight:searchDataSources",
"quicksight:searchFolders",
"quicksight:searchGroups",
"ram:getPermission",
"ram:getResourceShareAssociations",
"ram:getResourceShareInvitations",
"ram:getResourceShares",
"ram:listPendingInvitationResources",
"ram:listPrincipals",
"ram:listResources",
"ram:listResourceSharePermissions",
"rbin:getRule",
"rbin:listRules",
"rds:describeAccountAttributes",
"rds:describeBlueGreenDeployments",
"rds:describeCertificates",
```

```
"rds:describeDBClusterEndpoints",
"rds:describeDBClusterParameterGroups",
"rds:describeDBClusterParameters",
"rds:describeDBClusters",
"rds:describeDBClusterSnapshots",
"rds:describeDBEngineVersions",
"rds:describeDBInstanceAutomatedBackups",
"rds:describeDBInstances",
"rds:describeDBLogFiles",
"rds:describeDBParameterGroups",
"rds:describeDBParameters",
"rds:describeDBSecurityGroups",
"rds:describeDBSnapshotAttributes",
"rds:describeDBSnapshots",
"rds:describeDBSubnetGroups",
"rds:describeEngineDefaultClusterParameters",
"rds:describeEngineDefaultParameters",
"rds:describeEventCategories",
"rds:describeEvents",
"rds:describeEventSubscriptions",
"rds:describeExportTasks",
"rds:describeGlobalClusters",
"rds:describeIntegrations",
"rds:describeOptionGroupOptions",
"rds:describeOptionGroups",
"rds:describeOrderableDBInstanceOptions",
"rds:describePendingMaintenanceActions",
"rds:describeReservedDBInstances",
"rds:describeReservedDBInstancesOfferings",
"rds:describeSourceRegions",
"rds:describeValidDBInstanceModifications",
"rds:listTagsForResource",
"redshift-data:describeStatement",
"redshift-data:listStatements",
"redshift:describeClusterParameterGroups",
"redshift:describeClusterParameters",
"redshift:describeClusters",
"redshift:describeClusterSecurityGroups",
"redshift:describeClusterSnapshots",
"redshift:describeClusterSubnetGroups",
"redshift:describeClusterVersions",
"redshift:describeDataShares",
"redshift:describeDataSharesForConsumer",
"redshift:describeDataSharesForProducer",
```

```
"redshift:describeDefaultClusterParameters",
"redshift:describeEventCategories",
"redshift:describeEvents",
"redshift:describeEventSubscriptions",
"redshift:describeHsmClientCertificates",
"redshift:describeHsmConfigurations",
"redshift:describeLoggingStatus",
"redshift:describeOrderableClusterOptions",
"redshift:describeReservedNodeOfferings",
"redshift:describeReservedNodes",
"redshift:describeResize",
"redshift:describeSnapshotCopyGrants",
"redshift:describeStorage",
"redshift:describeTableRestoreStatus",
"redshift:describeTags",
"redshift-serverless:getEndpointAccess",
"redshift-serverless:getNamespace",
"redshift-serverless:getRecoveryPoint",
"redshift-serverless:getSnapshot",
"redshift-serverless:getTableRestoreStatus",
"redshift-serverless:getUsageLimit",
"redshift-serverless:getWorkgroup",
"redshift-serverless:listEndpointAccess",
"redshift-serverless:listNamespaces",
"redshift-serverless:listRecoveryPoints",
"redshift-serverless:listSnapshots",
"redshift-serverless:listTableRestoreStatus",
"redshift-serverless:listUsageLimits",
"redshift-serverless:listWorkgroups",
"rekognition:listCollections",
"rekognition:listFaces",
"resource-explorer-2:getAccountLevelServiceConfiguration",
"resource-explorer-2:getIndex",
"resource-explorer-2:getView",
"resource-explorer-2:listIndexes",
"resource-explorer-2:listViews",
"resource-explorer-2:search",
"resource-groups:getGroup",
"resource-groups:getGroupQuery",
"resource-groups:getTags",
"resource-groups:listGroupResources",
"resource-groups:listGroups",
"resource-groups:searchResources",
"robomaker:batchDescribeSimulationJob",
```

```
"robomaker:describeDeploymentJob",
"robomaker:describeFleet",
"robomaker:describeRobot",
"robomaker:describeRobotApplication",
"robomaker:describeSimulationApplication",
"robomaker:describeSimulationJob",
"robomaker:listDeploymentJobs",
"robomaker:listFleets",
"robomaker:listRobotApplications",
"robomaker:listRobots",
"robomaker:listSimulationApplications",
"robomaker:listSimulationJobs",
"route53-recovery-cluster:getRoutingControlState",
"route53-recovery-cluster:listRoutingControls",
"route53-recovery-control-config:describeControlPanel",
"route53-recovery-control-config:describeRoutingControl",
"route53-recovery-control-config:describeSafetyRule",
"route53-recovery-control-config:listControlPanels",
"route53-recovery-control-config:listRoutingControls",
"route53-recovery-control-config:listSafetyRules",
"route53-recovery-readiness:getCell",
"route53-recovery-readiness:getCellReadinessSummary",
"route53-recovery-readiness:getReadinessCheck",
"route53-recovery-readiness:getReadinessCheckResourceStatus",
"route53-recovery-readiness:getReadinessCheckStatus",
"route53-recovery-readiness:getRecoveryGroup",
"route53-recovery-readiness:getRecoveryGroupReadinessSummary",
"route53-recovery-readiness:listCells",
"route53-recovery-readiness:listReadinessChecks",
"route53-recovery-readiness:listRecoveryGroups",
"route53-recovery-readiness:listResourceSets",
"route53:getAccountLimit",
"route53:getChange",
"route53:getCheckerIpRanges",
"route53:getDNSSEC",
"route53:getGeoLocation",
"route53:getHealthCheck",
"route53:getHealthCheckCount",
"route53:getHealthCheckLastFailureReason",
"route53:getHealthCheckStatus",
"route53:getHostedZone",
"route53:getHostedZoneCount",
"route53:getHostedZoneLimit",
"route53:getQueryLoggingConfig",
```

```
"route53:getReusableDelegationSet",
"route53:getTrafficPolicy",
"route53:getTrafficPolicyInstance",
"route53:getTrafficPolicyInstanceCount",
"route53:listCidrBlocks",
"route53:listCidrCollections",
"route53:listCidrLocations",
"route53:listGeoLocations",
"route53:listHealthChecks",
"route53:listHostedZones",
"route53:listHostedZonesByName",
"route53:listHostedZonesByVpc",
"route53:listQueryLoggingConfigs",
"route53:listResourceRecordSets",
"route53:listReusableDelegationSets",
"route53:listTrafficPolicies",
"route53:listTrafficPolicyInstances",
"route53:listTrafficPolicyInstancesByHostedZone",
"route53:listTrafficPolicyInstancesByPolicy",
"route53:listTrafficPolicyVersions",
"route53:listVPCAssociationAuthorizations",
"route53domains:checkDomainAvailability",
"route53domains:getContactReachabilityStatus",
"route53domains:getDomainDetail",
"route53domains:getOperationDetail",
"route53domains:listDomains",
"route53domains:listOperations",
"route53domains:listPrices",
"route53domains:listTagsForDomain",
"route53domains:viewBilling",
"route53resolver:getFirewallConfig",
"route53resolver:getFirewallDomainList",
"route53resolver:getFirewallRuleGroup",
"route53resolver:getFirewallRuleGroupAssociation",
"route53resolver:getFirewallRuleGroupPolicy",
"route53resolver:getOutpostResolver",
"route53resolver:getResolverDnssecConfig",
"route53resolver:getResolverQueryLogConfig",
"route53resolver:getResolverQueryLogConfigAssociation",
"route53resolver:getResolverQueryLogConfigPolicy",
"route53resolver:getResolverRule",
"route53resolver:getResolverRuleAssociation",
"route53resolver:getResolverRulePolicy",
"route53resolver:listFirewallConfigs",
```



```
"route53resolver:listFirewallDomainLists",
"route53resolver:listFirewallDomains",
"route53resolver:listFirewallRuleGroupAssociations",
"route53resolver:listFirewallRuleGroups",
"route53resolver:listFirewallRules",
"route53resolver:listOutpostResolvers",
"route53resolver:listResolverConfigs",
"route53resolver:listResolverDnssecConfigs",
"route53resolver:listResolverEndpointIpAddresses",
"route53resolver:listResolverEndpoints",
"route53resolver:listResolverQueryLogConfigAssociations",
"route53resolver:listResolverQueryLogConfigs",
"route53resolver:listResolverRuleAssociations",
"route53resolver:listResolverRules",
"route53resolver:listTagsForResource",
"rum:batchGetRumMetricDefinitions",
"rum:getAppMonitor",
"rum:listAppMonitors",
"rum:listRumMetricsDestinations",
"s3:describeJob",
"s3:describeMultiRegionAccessPointOperation",
"s3:getAccelerateConfiguration",
"s3:getAccessPoint",
"s3:getAccessPointConfigurationForObjectLambda",
"s3:getAccessPointForObjectLambda",
"s3:getAccessPointPolicy",
"s3:getAccessPointPolicyForObjectLambda",
"s3:getAccessPointPolicyStatus",
"s3:getAccessPointPolicyStatusForObjectLambda",
"s3:getAccountPublicAccessBlock",
"s3:getAnalyticsConfiguration",
"s3:getBucketAcl",
"s3:getBucketCORS",
"s3:getBucketLocation",
"s3:getBucketLogging",
"s3:getBucketNotification",
"s3:getBucketObjectLockConfiguration",
"s3:getBucketOwnershipControls",
"s3:getBucketPolicy",
"s3:getBucketPolicyStatus",
"s3:getBucketPublicAccessBlock",
"s3:getBucketRequestPayment",
"s3:getBucketVersioning",
"s3:getBucketWebsite",
```

```
"s3:getEncryptionConfiguration",
"s3:getIntelligentTieringConfiguration",
"s3:getInventoryConfiguration",
"s3:getLifecycleConfiguration",
"s3:getMetricsConfiguration",
"s3:getMultiRegionAccessPoint",
"s3:getMultiRegionAccessPointPolicy",
"s3:getMultiRegionAccessPointPolicyStatus",
"s3:getMultiRegionAccessPointRoutes",
"s3:getObjectLegalHold",
"s3:getObjectRetention",
"s3:getReplicationConfiguration",
"s3:getStorageLensConfiguration",
"s3:listAccessPoints",
"s3:listAccessPointsForObjectLambda",
"s3:listAllMyBuckets",
"s3:listBucket",
"s3:listBucketMultipartUploads",
"s3:listBucketVersions",
"s3:listJobs",
"s3:listMultipartUploadParts",
"s3:listMultiRegionAccessPoints",
"s3:listStorageLensConfigurations",
"s3express:getBucketPolicy",
"s3express:listAllMyDirectoryBuckets",
"sagemaker:describeAction",
"sagemaker:describeAlgorithm",
"sagemaker:describeApp",
"sagemaker:describeAppImageConfig",
"sagemaker:describeArtifact",
"sagemaker:describeAutoMLJob",
"sagemaker:describeCluster",
"sagemaker:describeClusterNode",
"sagemaker:describeCodeRepository",
"sagemaker:describeCompilationJob",
"sagemaker:describeContext",
"sagemaker:describeDataQualityJobDefinition",
"sagemaker:describeDevice",
"sagemaker:describeDeviceFleet",
"sagemaker:describeDomain",
"sagemaker:describeEdgeDeploymentPlan",
"sagemaker:describeEdgePackagingJob",
"sagemaker:describeEndpoint",
"sagemaker:describeEndpointConfig",
```

```
"sagemaker:describeExperiment",
"sagemaker:describeFeatureGroup",
"sagemaker:describeFeatureMetadata",
"sagemaker:describeFlowDefinition",
"sagemaker:describeHub",
"sagemaker:describeHubContent",
"sagemaker:describeHumanTaskUi",
"sagemaker:describeHyperParameterTuningJob",
"sagemaker:describeImage",
"sagemaker:describeImageVersion",
"sagemaker:describeInferenceComponent",
"sagemaker:describeInferenceExperiment",
"sagemaker:describeInferenceRecommendationsJob",
"sagemaker:describeLabelingJob",
"sagemaker:describeModel",
"sagemaker:describeModelBiasJobDefinition",
"sagemaker:describeModelCard",
"sagemaker:describeModelCardExportJob",
"sagemaker:describeModelExplainabilityJobDefinition",
"sagemaker:describeModelPackage",
"sagemaker:describeModelPackageGroup",
"sagemaker:describeModelQualityJobDefinition",
"sagemaker:describeMonitoringSchedule",
"sagemaker:describeNotebookInstance",
"sagemaker:describeNotebookInstanceLifecycleConfig",
"sagemaker:describePipeline",
"sagemaker:describePipelineDefinitionForExecution",
"sagemaker:describePipelineExecution",
"sagemaker:describeProcessingJob",
"sagemaker:describeProject",
"sagemaker:describeSpace",
"sagemaker:describeStudioLifecycleConfig",
"sagemaker:describeSubscribedWorkteam",
"sagemaker:describeTrainingJob",
"sagemaker:describeTransformJob",
"sagemaker:describeTrial",
"sagemaker:describeTrialComponent",
"sagemaker:describeUserProfile",
"sagemaker:describeWorkforce",
"sagemaker:describeWorkteam",
"sagemaker:getDeviceFleetReport",
"sagemaker:getModelPackageGroupPolicy",
"sagemaker:getSagemakerServicecatalogPortfolioStatus",
"sagemaker:listActions",
```

```
"sagemaker:listAlgorithms",
"sagemaker:listAliases",
"sagemaker:listAppImageConfigs",
"sagemaker:listApps",
"sagemaker:listArtifacts",
"sagemaker:listAssociations",
"sagemaker:listAutoMLJobs",
"sagemaker:listCandidatesForAutoMLJob",
"sagemaker:listClusterNodes",
"sagemaker:listClusters",
"sagemaker:listCodeRepositories",
"sagemaker:listCompilationJobs",
"sagemaker:listContexts",
"sagemaker:listDataQualityJobDefinitions",
"sagemaker:listDeviceFleets",
"sagemaker:listDevices",
"sagemaker:listDomains",
"sagemaker:listEdgeDeploymentPlans",
"sagemaker:listEdgePackagingJobs",
"sagemaker:listEndpointConfigs",
"sagemaker:listEndpoints",
"sagemaker:listExperiments",
"sagemaker:listFeatureGroups",
"sagemaker:listFlowDefinitions",
"sagemaker:listHubContents",
"sagemaker:listHubContentVersions",
"sagemaker:listHubs",
"sagemaker:listHumanTaskUis",
"sagemaker:listHyperParameterTuningJobs",
"sagemaker:listImages",
"sagemaker:listImageVersions",
"sagemaker:listInferenceComponents",
"sagemaker:listInferenceExperiments",
"sagemaker:listInferenceRecommendationsJobs",
"sagemaker:listInferenceRecommendationsJobSteps",
"sagemaker:listLabelingJobs",
"sagemaker:listLabelingJobsForWorkteam",
"sagemaker:listLineageGroups",
"sagemaker:listModelBiasJobDefinitions",
"sagemaker:listModelCardExportJobs",
"sagemaker:listModelCards",
"sagemaker:listModelCardVersions",
"sagemaker:listModelExplainabilityJobDefinitions",
"sagemaker:listModelMetadata",
```

```
"sagemaker:listModelPackageGroups",
"sagemaker:listModelPackages",
"sagemaker:listModelQualityJobDefinitions",
"sagemaker:listModels",
"sagemaker:listMonitoringAlertHistory",
"sagemaker:listMonitoringAlerts",
"sagemaker:listMonitoringExecutions",
"sagemaker:listMonitoringSchedules",
"sagemaker:listNotebookInstanceLifecycleConfigs",
"sagemaker:listNotebookInstances",
"sagemaker:listPipelineExecutions",
"sagemaker:listPipelineExecutionSteps",
"sagemaker:listPipelineParametersForExecution",
"sagemaker:listPipelines",
"sagemaker:listProcessingJobs",
"sagemaker:listProjects",
"sagemaker:listSpaces",
"sagemaker:listStageDevices",
"sagemaker:listStudioLifecycleConfigs",
"sagemaker:listSubscribedWorkteams",
"sagemaker:listTags",
"sagemaker:listTrainingJobs",
"sagemaker:listTrainingJobsForHyperParameterTuningJob",
"sagemaker:listTransformJobs",
"sagemaker:listTrialComponents",
"sagemaker:listTrials",
"sagemaker:listUserProfiles",
"sagemaker:listWorkforces",
"sagemaker:listWorkteams",
"savingsplans:describeSavingsPlans",
"scheduler:getSchedule",
"scheduler:getScheduleGroup",
"scheduler:listScheduleGroups",
"scheduler:listSchedules",
"schemas:describeCodeBinding",
"schemas:describeDiscoverer",
"schemas:describeRegistry",
"schemas:describeSchema",
"schemas:getCodeBindingSource",
"schemas:getDiscoveredSchema",
"schemas:getResourcePolicy",
"schemas:listDiscoverers",
"schemas:listRegistries",
"schemas:listSchemas",
```

```
"schemas:listSchemaVersions",
"sdb:domainMetadata",
"sdb:listDomains",
"secretsmanager:describeSecret",
"secretsmanager:getResourcePolicy",
"secretsmanager:listSecrets",
"secretsmanager:listSecretVersionIds",
"securityhub:getEnabledStandards",
"securityhub:getFindings",
"securityhub:getInsightResults",
"securityhub:getInsights",
"securityhub:getMasterAccount",
"securityhub:getMembers",
"securityhub:listEnabledProductsForImport",
"securityhub:listInvitations",
"securityhub:listMembers",
"securitylake:getDataLakeExceptionSubscription",
"securitylake:getDataLakeOrganizationConfiguration",
"securitylake:getDataLakeSources",
"securitylake:getSubscriber",
"securitylake:listDataLakeExceptions",
"securitylake:listDataLakes",
"securitylake:listLogSources",
"securitylake:listSubscribers",
"serverlessrepo:getApplication",
"serverlessrepo:getApplicationPolicy",
"serverlessrepo:getCloudFormationTemplate",
"serverlessrepo:listApplicationDependencies",
"serverlessrepo:listApplications",
"serverlessrepo:listApplicationVersions",
"servicecatalog:describeConstraint",
"servicecatalog:describePortfolio",
"servicecatalog:describeProduct",
"servicecatalog:describeProductAsAdmin",
"servicecatalog:describeProductView",
"servicecatalog:describeProvisioningArtifact",
"servicecatalog:describeProvisioningParameters",
"servicecatalog:describeRecord",
"servicecatalog:listAcceptedPortfolioShares",
"servicecatalog:listConstraintsForPortfolio",
"servicecatalog:listLaunchPaths",
"servicecatalog:listPortfolioAccess",
"servicecatalog:listPortfolios",
"servicecatalog:listPortfoliosForProduct",
```

```
"servicecatalog:listPrincipalsForPortfolio",
"servicecatalog:listProvisioningArtifacts",
"servicecatalog:listRecordHistory",
"servicecatalog:scanProvisionedProducts",
"servicecatalog:searchProducts",
"servicequotas:getAssociationForServiceQuotaTemplate",
"servicequotas:getAWSDefaultServiceQuota",
"servicequotas:getRequestedServiceQuotaChange",
"servicequotas:getServiceQuota",
"servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:listAWSDefaultServiceQuotas",
"servicequotas:listRequestedServiceQuotaChangeHistory",
"servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:listServiceQuotas",
"servicequotas:listServices",
"ses:describeActiveReceiptRuleSet",
"ses:describeConfigurationSet",
"ses:describeReceiptRule",
"ses:describeReceiptRuleSet",
"ses:getAccount",
"ses:getAccountSendingEnabled",
"ses:getBlacklistReports",
"ses:getConfigurationSet",
"ses:getConfigurationSetEventDestinations",
"ses:getContactList",
"ses:getDedicatedIp",
"ses:getDedicatedIpPool",
"ses:getDedicatedIps",
"ses:getDeliverabilityDashboardOptions",
"ses:getDeliverabilityTestReport",
"ses:getDomainDeliverabilityCampaign",
"ses:getDomainStatisticsReport",
"ses:getEmailIdentity",
"ses:getIdentityDkimAttributes",
"ses:getIdentityMailFromDomainAttributes",
"ses:getIdentityNotificationAttributes",
"ses:getIdentityPolicies",
"ses:getIdentityVerificationAttributes",
"ses:getImportJob",
"ses:getSendQuota",
"ses:getSendStatistics",
"ses:listConfigurationSets",
"ses:listContactLists",
```

```
"ses:listContacts",
"ses:listCustomVerificationEmailTemplates",
"ses:listDedicatedIpPools",
"ses:listDeliverabilityTestReports",
"ses:listDomainDeliverabilityCampaigns",
"ses:listEmailIdentities",
"ses:listEmailTemplates",
"ses:listIdentities",
"ses:listIdentityPolicies",
"ses:listImportJobs",
"ses:listReceiptFilters",
"ses:listReceiptRuleSets",
"ses:listRecommendations",
"ses:listTagsForResource",
"ses:listTemplates",
"ses:listVerifiedEmailAddresses",
"shield:describeAttack",
"shield:describeProtection",
"shield:describeSubscription",
"shield:listAttacks",
"shield:listProtections",
"sms-voice:getConfigurationSetEventDestinations",
"sms:getConnectors",
"sms:getReplicationJobs",
"sms:getReplicationRuns",
"sms:getServers",
"snowball:describeAddress",
"snowball:describeAddresses",
"snowball:describeJob",
"snowball:getSnowballUsage",
"snowball:listJobs",
"snowball:listServiceVersions",
"sns:checkIfPhoneNumberIsOptedOut",
"sns:getDataProtectionPolicy",
"sns:getEndpointAttributes",
"sns:getPlatformApplicationAttributes",
"sns:getSMSAttributes",
"sns:getSMSSandboxAccountStatus",
"sns:getSubscriptionAttributes",
"sns:getTopicAttributes",
"sns:listEndpointsByPlatformApplication",
"sns:listOriginationNumbers",
"sns:listPhoneNumbersOptedOut",
"sns:listPlatformApplications",
```



```
"sns:listSMSSandboxPhoneNumbers",
"sns:listSubscriptions",
"sns:listSubscriptionsByTopic",
"sns:listTopics",
"sqs:getQueueAttributes",
"sqs:getQueueUrl",
"sqs:listDeadLetterSourceQueues",
"sqs:listQueues",
"ssm-contacts:describeEngagement",
"ssm-contacts:describePage",
"ssm-contacts:getContact",
"ssm-contacts:getContactChannel",
"ssm-contacts:getContactPolicy",
"ssm-contacts:getRotation",
"ssm-contacts:getRotationOverride",
"ssm-contacts:listContactChannels",
"ssm-contacts:listContacts",
"ssm-contacts:listEngagements",
"ssm-contacts:listPageReceipts",
"ssm-contacts:listPageResolutions",
"ssm-contacts:listPagesByContact",
"ssm-contacts:listPagesByEngagement",
"ssm-contacts:listPreviewRotationShifts",
"ssm-contacts:listRotationOverrides",
"ssm-contacts:listRotations",
"ssm-contacts:listRotationShifts",
"ssm-incidents:getIncidentRecord",
"ssm-incidents:getReplicationSet",
"ssm-incidents:getResourcePolicies",
"ssm-incidents:getResponsePlan",
"ssm-incidents:getTimelineEvent",
"ssm-incidents:listIncidentRecords",
"ssm-incidents:listRelatedItems",
"ssm-incidents:listReplicationSets",
"ssm-incidents:listResponsePlans",
"ssm-incidents:listTimelineEvents",
"ssm-sap:getApplication",
"ssm-sap:getComponent",
"ssm-sap:getDatabase",
"ssm-sap:getOperation",
"ssm-sap:getResourcePermission",
"ssm-sap:listApplications",
"ssm-sap:listComponents",
"ssm-sap:listDatabases",
```

```
"ssm-sap:listOperations",
"ssm:describeActivations",
"ssm:describeAssociation",
"ssm:describeAssociationExecutions",
"ssm:describeAssociationExecutionTargets",
"ssm:describeAutomationExecutions",
"ssm:describeAutomationStepExecutions",
"ssm:describeAvailablePatches",
"ssm:describeDocument",
"ssm:describeDocumentPermission",
"ssm:describeEffectiveInstanceAssociations",
"ssm:describeEffectivePatchesForPatchBaseline",
"ssm:describeInstanceAssociationsStatus",
"ssm:describeInstanceInformation",
"ssm:describeInstancePatches",
"ssm:describeInstancePatchStates",
"ssm:describeInstancePatchStatesForPatchGroup",
"ssm:describeInventoryDeletions",
"ssm:describeMaintenanceWindowExecutions",
"ssm:describeMaintenanceWindowExecutionTaskInvocations",
"ssm:describeMaintenanceWindowExecutionTasks",
"ssm:describeMaintenanceWindows",
"ssm:describeMaintenanceWindowSchedule",
"ssm:describeMaintenanceWindowsForTarget",
"ssm:describeMaintenanceWindowTargets",
"ssm:describeMaintenanceWindowTasks",
"ssm:describeOpsItems",
"ssm:describeParameters",
"ssm:describePatchBaselines",
"ssm:describePatchGroups",
"ssm:describePatchGroupState",
"ssm:describePatchProperties",
"ssm:describeSessions",
"ssm:getAutomationExecution",
"ssm:getCalendarState",
"ssm:getCommandInvocation",
"ssm:getConnectionStatus",
"ssm:getDefaultPatchBaseline",
"ssm:getDeployablePatchSnapshotForInstance",
"ssm:getInventorySchema",
"ssm:getMaintenanceWindow",
"ssm:getMaintenanceWindowExecution",
"ssm:getMaintenanceWindowExecutionTask",
"ssm:getMaintenanceWindowExecutionTaskInvocation",
```

```
"ssm:getMaintenanceWindowTask",
"ssm:getOpsItem",
"ssm:getOpsMetadata",
"ssm:getOpsSummary",
"ssm:getPatchBaseline",
"ssm:getPatchBaselineForPatchGroup",
"ssm:getResourcePolicies",
"ssm:getServiceSetting",
"ssm:listAssociations",
"ssm:listAssociationVersions",
"ssm:listCommandInvocations",
"ssm:listCommands",
"ssm:listComplianceItems",
"ssm:listComplianceSummaries",
"ssm:listDocuments",
"ssm:listDocumentMetadataHistory",
"ssm:listDocumentVersions",
"ssm:listOpsItemEvents",
"ssm:listOpsItemRelatedItems",
"ssm:listOpsMetadata",
"ssm:listResourceComplianceSummaries",
"ssm:listResourceDataSync",
"ssm:listTagsForResource",
"sso:describeApplicationAssignment",
"sso:describeApplicationProvider",
"sso:describeApplication",
"sso:describeInstance",
"sso:describeTrustedTokenIssuer",
"sso:getApplicationAccessScope",
"sso:getApplicationAssignmentConfiguration",
"sso:getApplicationAuthenticationMethod",
"sso:getApplicationGrant",
"sso:getApplicationInstance",
"sso:getApplicationTemplate",
"sso:getManagedApplicationInstance",
"sso:getSharedSsoConfiguration",
"sso:listApplicationAccessScopes",
"sso:listApplicationAssignments",
"sso:listApplicationAuthenticationMethods",
"sso:listApplicationGrants",
"sso:listApplicationInstances",
"sso:listApplicationProviders",
"sso:listApplications",
"sso:listApplicationTemplates",
```

```
"sso:listDirectoryAssociations",
"sso:listInstances",
"sso:listProfileAssociations",
"sso:listTrustedTokenIssuers",
"states:describeActivity",
"states:describeExecution",
"states:describeMapRun",
"states:describeStateMachine",
"states:describeStateMachineAlias",
"states:describeStateMachineForExecution",
"states:getExecutionHistory",
"states:listActivities",
"states:listExecutions",
"states:listMapRuns",
"states:listStateMachineAliases",
"states:listStateMachines",
"states:listStateMachineVersions",
"storagegateway:describeBandwidthRateLimit",
"storagegateway:describeCache",
"storagegateway:describeCachediSCSIVolumes",
"storagegateway:describeFileSystemAssociations",
"storagegateway:describeGatewayInformation",
"storagegateway:describeMaintenanceStartTime",
"storagegateway:describeNFSFileShares",
"storagegateway:describeSMBFileShares",
"storagegateway:describeSMBSettings",
"storagegateway:describeSnapshotSchedule",
"storagegateway:describeStorediSCSIVolumes",
"storagegateway:describeTapeArchives",
"storagegateway:describeTapeRecoveryPoints",
"storagegateway:describeTapes",
"storagegateway:describeUploadBuffer",
"storagegateway:describeVTLDevices",
"storagegateway:describeWorkingStorage",
"storagegateway:listAutomaticTapeCreationPolicies",
"storagegateway:listFileShares",
"storagegateway:listFileSystemAssociations",
"storagegateway:listGateways",
"storagegateway:listLocalDisks",
"storagegateway:listTagsForResource",
"storagegateway:listTapes",
"storagegateway:listVolumeInitiators",
"storagegateway:listVolumeRecoveryPoints",
"storagegateway:listVolumes",
```

```
"swf:countClosedWorkflowExecutions",
"swf:countOpenWorkflowExecutions",
"swf:countPendingActivityTasks",
"swf:countPendingDecisionTasks",
"swf:describeActivityType",
"swf:describeDomain",
"swf:describeWorkflowExecution",
"swf:describeWorkflowType",
"swf:getWorkflowExecutionHistory",
"swf:listActivityTypes",
"swf:listClosedWorkflowExecutions",
"swf:listDomains",
"swf:listOpenWorkflowExecutions",
"swf:listWorkflowTypes",
"synthetics:describeCanaries",
"synthetics:describeCanariesLastRun",
"synthetics:describeRuntimeVersions",
"synthetics:getCanary",
"synthetics:getCanaryRuns",
"synthetics:getGroup",
"synthetics:listAssociatedGroups",
"synthetics:listGroupResources",
"synthetics:listGroups",
"tiros:createQuery",
"tiros:getQueryAnswer",
"tiros:getQueryExplanation",
"transcribe:describeLanguageModel",
"transcribe:getCallAnalyticsCategory",
"transcribe:getCallAnalyticsJob",
"transcribe:getMedicalTranscriptionJob",
"transcribe:getMedicalVocabulary",
"transcribe:getTranscriptionJob",
"transcribe:getVocabulary",
"transcribe:getVocabularyFilter",
"transcribe:listCallAnalyticsCategories",
"transcribe:listCallAnalyticsJobs",
"transcribe:listLanguageModels",
"transcribe:listMedicalTranscriptionJobs",
"transcribe:listMedicalVocabularies",
"transcribe:listTranscriptionJobs",
"transcribe:listVocabularies",
"transcribe:listVocabularyFilters",
"transfer:describeAccess",
"transfer:describeAgreement",
```

```
"transfer:describeConnector",
"transfer:describeExecution",
"transfer:describeProfile",
"transfer:describeServer",
"transfer:describeUser",
"transfer:describeWorkflow",
"transfer:listAccesses",
"transfer:listAgreements",
"transfer:listConnectors",
"transfer:listExecutions",
"transfer:listHostKeys",
"transfer:listProfiles",
"transfer:listServers",
"transfer:listTagsForResource",
"transfer:listUsers",
"transfer:listWorkflows",
"transfer:sendWorkflowStepState",
"trustedadvisor:getOrganizationRecommendation",
"trustedadvisor:getRecommendation",
"trustedadvisor:listChecks",
"trustedadvisor:listOrganizationRecommendationAccounts",
"trustedadvisor:listOrganizationRecommendationResources",
"trustedadvisor:listOrganizationRecommendations",
"trustedadvisor:listRecommendationResources",
"trustedadvisor:listRecommendations",
"verifiedpermissions:getIdentitySource",
"verifiedpermissions:getPolicy",
"verifiedpermissions:getPolicyStore",
"verifiedpermissions:getPolicyTemplate",
"verifiedpermissions:getSchema",
"verifiedpermissions:listIdentitySources",
"verifiedpermissions:listPolicies",
"verifiedpermissions:listPolicyStores",
"verifiedpermissions:listPolicyTemplates",
"vpc-lattice:getAccessLogSubscription",
"vpc-lattice:getAuthPolicy",
"vpc-lattice:getListener",
"vpc-lattice:getResourcePolicy",
"vpc-lattice:getRule",
"vpc-lattice:getService",
"vpc-lattice:getServiceNetwork",
"vpc-lattice:getServiceNetworkServiceAssociation",
"vpc-lattice:getServiceNetworkVpcAssociation",
"vpc-lattice:getTargetGroup",
```

```
"vpc-lattice:listAccessLogSubscriptions",
"vpc-lattice:listListeners",
"vpc-lattice:listRules",
"vpc-lattice:listServiceNetworks",
"vpc-lattice:listServiceNetworkServiceAssociations",
"vpc-lattice:listServiceNetworkVpcAssociations",
"vpc-lattice:listServices",
"vpc-lattice:listTargetGroups",
"vpc-lattice:listTargets",
"waf-regional:getByteMatchSet",
"waf-regional:getChangeTokenStatus",
"waf-regional:getGeoMatchSet",
"waf-regional:getIPSet",
"waf-regional:getLoggingConfiguration",
"waf-regional:getRateBasedRule",
"waf-regional:getRegexMatchSet",
"waf-regional:getRegexPatternSet",
"waf-regional:getRule",
"waf-regional:getRuleGroup",
"waf-regional:getSqlInjectionMatchSet",
"waf-regional:getWebACL",
"waf-regional:getWebACLForResource",
"waf-regional:listActivatedRulesInRuleGroup",
"waf-regional:listByteMatchSets",
"waf-regional:listGeoMatchSets",
"waf-regional:listIPSets",
"waf-regional:listLoggingConfigurations",
"waf-regional:listRateBasedRules",
"waf-regional:listRegexMatchSets",
"waf-regional:listRegexPatternSets",
"waf-regional:listResourcesForWebACL",
"waf-regional:listRuleGroups",
"waf-regional:listRules",
"waf-regional:listSqlInjectionMatchSets",
"waf-regional:listWebACLs",
"waf:getByteMatchSet",
"waf:getChangeTokenStatus",
"waf:getGeoMatchSet",
"waf:getIPSet",
"waf:getLoggingConfiguration",
"waf:getRateBasedRule",
"waf:getRegexMatchSet",
"waf:getRegexPatternSet",
"waf:getRule",
```

```
"waf:getRuleGroup",
"waf:getSampledRequests",
"waf:getSizeConstraintSet",
"waf:getSqlInjectionMatchSet",
"waf:getWebACL",
"waf:getXssMatchSet",
"waf:listActivatedRulesInRuleGroup",
"waf:listByteMatchSets",
"waf:listGeoMatchSets",
"waf:listIPSets",
"waf:listLoggingConfigurations",
"waf:listRateBasedRules",
"waf:listRegexMatchSets",
"waf:listRegexPatternSets",
"waf:listRuleGroups",
"waf:listRules",
"waf:listSizeConstraintSets",
"waf:listSqlInjectionMatchSets",
"waf:listWebACLs",
"waf:listXssMatchSets",
"wafv2:checkCapacity",
"wafv2:describeManagedRuleGroup",
"wafv2:getIPSet",
"wafv2:getLoggingConfiguration",
"wafv2:getPermissionPolicy",
"wafv2:getRateBasedStatementManagedKeys",
"wafv2:getRegexPatternSet",
"wafv2:getRuleGroup",
"wafv2:getSampledRequests",
"wafv2:getWebACL",
"wafv2:getWebACLForResource",
"wafv2:listAvailableManagedRuleGroups",
"wafv2:listIPSets",
"wafv2:listLoggingConfigurations",
"wafv2:listRegexPatternSets",
"wafv2:listResourcesForWebACL",
"wafv2:listRuleGroups",
"wafv2:listTagsForResource",
"wafv2:listWebACLs",
"workdocs:checkAlias",
"workdocs:describeAvailableDirectories",
"workdocs:describeInstances",
"workmail:describeGroup",
"workmail:describeOrganization",
```



```
    "workmail:describeResource",
    "workmail:describeUser",
    "workmail:listAliases",
    "workmail:listGroupMembers",
    "workmail:listGroups",
    "workmail:listMailboxPermissions",
    "workmail:listOrganizations",
    "workmail:listResourceDelegates",
    "workmail:listResources",
    "workmail:listUsers",
    "workspaces-web:getBrowserSettings",
    "workspaces-web:getIdentityProvider",
    "workspaces-web:getNetworkSettings",
    "workspaces-web:getPortal",
    "workspaces-web:getPortalServiceProviderMetadata",
    "workspaces-web:getTrustStoreCertificate",
    "workspaces-web:getUserSettings",
    "workspaces-web:listBrowserSettings",
    "workspaces-web:listIdentityProviders",
    "workspaces-web:listNetworkSettings",
    "workspaces-web:listPortals",
    "workspaces-web:listTagsForResource",
    "workspaces-web:listTrustStoreCertificates",
    "workspaces-web:listTrustStores",
    "workspaces-web:listUserSettings",
    "workspaces:describeAccount",
    "workspaces:describeAccountModifications",
    "workspaces:describeIpGroups",
    "workspaces:describeTags",
    "workspaces:describeWorkspaceBundles",
    "workspaces:describeWorkspaceDirectories",
    "workspaces:describeWorkspaceImages",
    "workspaces:describeWorkspaces",
    "workspaces:describeWorkspacesConnectionStatus",
    "xray:getEncryptionConfig",
    "xray:getGroup",
    "xray:getGroups",
    "xray:getSamplingRules",
    "xray:listResourcePolicies"
  ],
  "Effect" : "Allow",
  "Resource" : [
    "*"
  ]
]
```

```
    }  
  ],  
  "Version" : "2012-10-17"  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

説明： AWS AWS アカウント 情報を検出する Systems Manager (SSM) 許可を付与します。

AWSSystemsManagerAccountDiscoveryServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 10 月 24 日 17:21 UTC
- 編集日時: 2022 年 10 月 17 日 20:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSystemsManagerChangeManagementServicePolicy

説明： AWS Systems Manager 変更管理フレームワークによって管理または使用される AWS リソースへのアクセスを提供します。

AWSSystemsManagerChangeManagementServicePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 7 日 22:21 UTC
- 編集日時: 2020 年 12 月 7 日 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"  
    ]  
  }  
}  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSystemsManagerForSAPFullAccess

説明： AWS Systems Manager for SAP サービスへのフルアクセスを提供します

AWSSystemsManagerForSAPFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerForSAPFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2022 年 11 月 18 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSystemsManagerForSAPReadOnlyAccess

説明： AWS Systems Manager for SAP サービスへの読み取り専用アクセスを提供します

AWSSystemsManagerForSAPReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSSystemsManagerForSAPReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 17 日 02:11 UTC
- 編集日時: 2022 年 11 月 17 日 02:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```



```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

説明：SSM Explorer が OpsData 関連するオペレーションを管理するための IAM ロール

AWSSystemsManagerOpsDataSyncServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 4 月 26 日 20:42 UTC
- 編集日時: 2023 年 6 月 28 日 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

ポリシーのバージョニング

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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
      }
    }
  }
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxAssetServerPolicy

説明：このポリシーは、通常のオペレーションに必要なアクセス許可を AWS Portal アセットサーバーに付与します。

AWSThinkboxAssetServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAssetServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:18 UTC
- 編集日時: 2020 年 5 月 27 日 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxAWSPortalAdminPolicy

説明: このポリシーは、AWS ポータル管理の必要に応じて AWS Thinkbox の Deadline ソフトウェアに複数の AWS サービスへのフルアクセスを許可します。これには、複数の EC2 リソースタイプに任意のタグを作成するためのアクセス権限が含まれます。

AWSThinkboxAWSPortalAdminPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:41 UTC
- 編集日時: 2024 年 4 月 12 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
```



```
"ec2:DescribeInstanceTypeOfferings",
"ec2:DescribeRegions",
"ec2:DescribeSpotFleetRequestHistory",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSpotFleetInstances",
"ec2:DescribeSpotFleetRequests",
"ec2:DescribeSpotPriceHistory",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeVpcEndpoints",
"ec2:GetConsoleOutput",
"ec2:ImportKeyPair",
"ec2:ReleaseAddress",
"ec2:RequestSpotFleet",
"ec2:CancelSpotFleetRequests",
"ec2:DisassociateAddress",
"ec2>DeleteFleets",
"ec2>DeleteLaunchTemplate",
"ec2>DeleteVpc",
"ec2>DeletePlacementGroup",
"ec2>DeleteVpcEndpoints",
"ec2>DeleteInternetGateway",
"ec2>DeleteSecurityGroup",
"ec2:RevokeSecurityGroupIngress",
"ec2>DeleteRoute",
"ec2>DeleteRouteTable",
"ec2:DisassociateRouteTable",
"ec2>DeleteSubnet",
"ec2>DeleteNatGateway",
"ec2:DetachInternetGateway",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyFleet",
"ec2:ModifySpotFleetRequest",
"ec2:ModifyVpcAttribute"
],
"Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal2",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:key-pair/*",
```

```
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:placement-group/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:image/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal3",
  "Effect" : "Allow",
  "Action" : "ec2:RunInstances",
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:InstanceProfile" : "arn:aws:iam:*:*:instance-profile/AWSPortal*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal4",
  "Effect" : "Allow",
  "Action" : "ec2:TerminateInstances",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal5",
  "Effect" : "Allow",
  "Action" : "ec2:TerminateInstances",
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal6",
```

```
"Effect" : "Allow",
"Action" : "ec2:TerminateInstances",
"Resource" : "*",
"Condition" : {
  "StringLike" : {
    "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal7",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:instance/*",
  "Condition" : {
    "StringLike" : {
      "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal8",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal9",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal10",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetUser"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AWSThinkboxAWSPortal11",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetInstanceProfile"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:instance-profile/AWSPortal*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal12",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
    ],
    "Resource" : [
        "arn:aws:iam:*:*:policy/AWSPortal*"
    ]
},
{
    "Sid" : "AWSThinkboxAWSPortal13",
    "Effect" : "Allow",
    "Action" : [
        "iam:GetRole",
```

```
    "iam:GetRolePolicy"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal14",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/AWSPortal*",
    "arn:aws:iam::*:role/DeadlineSpot*"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com",
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxAWSPortal15",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "ec2fleet.amazonaws.com",
        "spot.amazonaws.com",
        "spotfleet.amazonaws.com"
      ]
    }
  }
},
}
```

```
{
  "Sid" : "AWSThinkboxAWSPortal16",
  "Effect" : "Allow",
  "Action" : [
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:PutBucketAcl",
    "s3:PutBucketCORS",
    "s3:PutBucketVersioning",
    "s3:GetBucketAcl",
    "s3:GetObject",
    "s3:PutBucketLogging",
    "s3:PutBucketTagging",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3>DeleteBucket",
    "s3>DeleteObject",
    "s3>DeleteBucketPolicy",
    "s3>DeleteObjectVersion"
  ],
  "Resource" : [
    "arn:aws:s3::*:awsportal*",
    "arn:aws:s3::*:stack*",
    "arn:aws:s3::*:aws-portal-cache*",
    "arn:aws:s3::*:logs-for-aws-portal-cache*",
    "arn:aws:s3::*:logs-for-stack*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal17",
  "Effect" : "Allow",
  "Action" : [
    "s3:PutBucketPolicy"
  ],
  "Resource" : [
    "arn:aws:s3::*:logs-for-aws-portal-cache*"
  ]
},
{
```

```
"Sid" : "AWSThinkboxAWSPortal18",
"Effect" : "Allow",
"Action" : [
  "s3:PutBucketOwnershipControls"
],
"Resource" : [
  "arn:aws:s3::*:logs-for-stack*"
],
},
{
  "Sid" : "AWSThinkboxAWSPortal19",
  "Effect" : "Allow",
  "Action" : [
    "s3:ListAllMyBuckets"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal20",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:Scan"
  ],
  "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
},
{
  "Sid" : "AWSThinkboxAWSPortal21",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:CreateStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResources",
    "cloudformation>DeleteStack",
    "cloudformation>DeleteChangeSet",
    "cloudformation:ListStackResources",
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:UpdateTerminationProtection",
    "cloudformation:TagResource",
    "cloudformation:UntagResource"
  ],
  "Resource" : [
    "arn:aws:cloudformation:*:*:stack/stack*/*"
  ],
```

```
    "arn:aws:cloudformation:*:*:stack/Deadline*/*"
  ]
},
{
  "Sid" : "AWSThinkboxAWSPortal22",
  "Effect" : "Allow",
  "Action" : [
    "cloudformation:EstimateTemplateCost",
    "cloudformation:DescribeStacks",
    "cloudformation:ListStacks"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal23",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogStreams",
    "logs:GetLogEvents",
    "logs:PutRetentionPolicy",
    "logs>DeleteRetentionPolicy"
  ],
  "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
},
{
  "Sid" : "AWSThinkboxAWSPortal24",
  "Effect" : "Allow",
  "Action" : [
    "logs:DescribeLogGroups",
    "logs>CreateLogGroup"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AWSThinkboxAWSPortal25",
  "Effect" : "Allow",
  "Action" : [
    "kms:Encrypt",
    "kms:GenerateDataKey"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
```



```
    "StringLike" : {
      "kms:ViaService" : [
        "s3.*.amazonaws.com",
        "secretsmanager.*.amazonaws.com"
      ]
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal26",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:CreateSecret"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "secretsmanager:Name" : [
          "rcs-tls-pw*"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxAWSPortal27",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:DeleteSecret",
      "secretsmanager:UpdateSecret",
      "secretsmanager:DescribeSecret",
      "secretsmanager:TagResource"
    ],
    "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxAWSPortalGatewayPolicy

説明：このポリシーは、通常のオペレーションに必要なアクセス許可を AWS Portal Gateway マシンに付与します。

AWSThinkboxAWSPortalGatewayPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalGatewayPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:05 UTC
- 編集日時: 2020 年 6 月 30 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
```

```
    "logs:DescribeLogGroups",
    "logs:CreateLogStream"
  ],
  "Resource" : [
    "arn:aws:logs:*:*:log-group:/thinkbox*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject",
    "s3:PutObject",
    "s3:ListBucket"
  ],
  "Resource" : [
    "arn:aws:s3:::aws-portal-cache*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : "dynamodb:Scan",
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:ListBucket",
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*"
  ]
},
}
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "s3:PutObject"
  ],
  "Resource" : [
    "arn:aws:s3:::stack*/gateway_certs/*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "secretsmanager:GetSecretValue"
  ],
  "Resource" : [
    "arn:aws:secretsmanager:*:*:secret:rds-tls-pw-stack*"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxAWSPortalWorkerPolicy

説明: このポリシーは、AWS ポータルの Deadline Workers に、通常のオペレーションに必要なアクセス許可を付与します。

AWSThinkboxAWSPortalWorkerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxAWSPortalWorkerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:15 UTC
- 編集日時: 2020 年 12 月 7 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

説明: AWS Thinkbox の Deadline Resource Tracker のオペレーションに必要なアクセス許可を付与します。これには、DeleteFleets や など、一部の EC2 アクションへのフルアクセスが含まれます CancelSpotFleetRequests。

AWSThinkboxDeadlineResourceTrackerAccessPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineResourceTrackerAccessPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:25 UTC
- 編集日時: 2020 年 5 月 27 日 19:25 UTC

- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineResourceTrackerAccessPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

説明: AWS Thinkbox の Deadline Resource Tracker を作成、破棄、管理するために必要なアクセス許可を付与します。

AWSThinkboxDeadlineResourceTrackerAdminPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineResourceTrackerAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:29 UTC
- 編集日時: 2024 年 4 月 12 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
```

```
    "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
  ],
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker4",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:CreateTable",
    "dynamodb>DeleteTable",
    "dynamodb:DescribeTable",
    "dynamodb:ListTagsOfResource",
    "dynamodb:TagResource",
    "dynamodb:UntagResource"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
    "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker5",
  "Effect" : "Allow",
  "Action" : [
    "dynamodb:BatchWriteItem",
    "dynamodb:Scan"
  ],
  "Resource" : [
    "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker6",
  "Effect" : "Allow",
  "Action" : [
    "events>DeleteRule",
    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource" : [
    "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
  ]
}
```

```
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker7",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetRole",
      "iam:ListAttachedRolePolicies"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DeadlineResourceTracker*"
    ]
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker8",
    "Effect" : "Allow",
    "Action" : [
      "iam:GetUser"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker9",
    "Effect" : "Allow",
    "Action" : [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:AWSServiceName" : [
          "dynamodb.application-autoscaling.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker10",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ]
  }
}
```

```
    ],
    "Resource" : [
      "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "lambda.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker11",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "application-autoscaling.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker12",
    "Effect" : "Allow",
    "Action" : [
      "lambda:GetEventSourceMapping"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "AWSThinkboxDeadlineResourceTracker13",
    "Effect" : "Allow",
    "Action" : [
```

```
    "lambda:CreateEventSourceMapping",
    "lambda>DeleteEventSourceMapping"
  ],
  "Resource" : [
    "*"
  ],
  "Condition" : {
    "StringLike" : {
      "lambda:FunctionArn" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    }
  }
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker14",
  "Effect" : "Allow",
  "Action" : [
    "lambda:AddPermission",
    "lambda:RemovePermission"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
  ],
  "Condition" : {
    "StringLike" : {
      "lambda:Principal" : "events.amazonaws.com"
    }
  }
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker15",
  "Effect" : "Allow",
  "Action" : [
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda>DeleteFunctionConcurrency",
    "lambda:GetFunction",
    "lambda:GetFunctionConfiguration",
    "lambda:ListTags",
    "lambda:PutFunctionConcurrency",
    "lambda:TagResource",
    "lambda:UntagResource",
    "lambda:UpdateFunctionCode",
```



```
    "lambda:UpdateFunctionConfiguration"
  ],
  "Resource" : [
    "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker16",
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*:/deadline_aws_resource_tracker-*.zip",
    "arn:aws:s3::*:/DeadlineAWSResourceTrackerTemplate-*.yaml"
  ]
},
{
  "Sid" : "AWSThinkboxDeadlineResourceTracker17",
  "Effect" : "Allow",
  "Action" : [
    "sqs:CreateQueue",
    "sqs>DeleteQueue",
    "sqs:GetQueueAttributes",
    "sqs:ListQueueTags",
    "sqs:TagQueue",
    "sqs:UntagQueue"
  ],
  "Resource" : [
    "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
    "arn:aws:sqs:*:*:DeadlineResourceTracker*"
  ]
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

説明： AWS Thinkbox の Deadline Spot Event Plugin に必要なアクセス許可を付与します。これには、スポットフリートをリクエスト、変更、キャンセルするアクセス許可と、制限された PassRole アクセス許可が含まれます。

AWSThinkboxDeadlineSpotEventPluginAdminPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineSpotEventPluginAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:38 UTC
- 編集日時: 2020 年 5 月 27 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

説明： AWS Thinkbox Deadline スポットイベントプラグインワーカーソフトウェアを実行する EC2 インスタンスに必要なアクセス許可を付与します。

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSThinkboxDeadlineSpotEventPluginWorkerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 27 日 19:35 UTC
- 編集日時: 2020 年 12 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTransferConsoleFullAccess

説明： 経由で AWS Transfer へのフルアクセスを提供します AWS Management Console

AWSTransferConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransferConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 14 日 19:33 UTC
- 編集日時: 2020 年 12 月 14 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTransferFullAccess

説明： AWS Transfer Service へのフルアクセスを提供します。

AWSTransferFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransferFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 14 日 19:37 UTC
- 編集日時: 2020 年 12 月 14 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTransferLoggingAccess

説明： AWS Transfer フルアクセスを許可してログストリームとグループを作成し、ログイベントをアカウントに配置

AWSTransferLoggingAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransferLoggingAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 1 月 14 日 15:32 UTC
- 編集日時: 2019 年 1 月 14 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTransferReadOnlyAccess

説明： AWS Transfer サービスへの読み取り専用アクセスを提供します。

AWSTransferReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTransferReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 27 日 17:54 UTC
- 編集日時: 2020 年 8 月 27 日 17:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSTrustedAdvisorPriorityFullAccess

説明： AWS Trusted Advisor Priority へのフルアクセスを提供します。このポリシーにより、ユーザーは Trusted Advisor を Organizations との信頼されたサービスとして追加し、Trusted Advisor Priority の委任管理者アカウントを指定することもできます。 AWS

AWSTrustedAdvisorPriorityFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSTrustedAdvisorPriorityFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 16 日 16:08 UTC
- 編集日時: 2022 年 8 月 16 日 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

説明： AWS Trusted Advisor Priority への読み取り専用アクセスを提供します。これには、委任管理者アカウントを閲覧する許可が含まれます。

AWSTrustedAdvisorPriorityReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSTrustedAdvisorPriorityReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 16 日 16:35 UTC
- 編集日時: 2022 年 8 月 16 日 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTrustedAdvisorReportingServiceRolePolicy

説明： Trusted Advisor マルチアカウントレポートのサービスポリシー

AWSTrustedAdvisorReportingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 19 日 17:41 UTC
- 編集日時: 2023 年 2 月 28 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSTrustedAdvisorServiceRolePolicy

説明: AWS Trusted Advisor Service へのアクセスにより、コストの削減、パフォーマンスの向上、AWS 環境のセキュリティの向上に役立ちます。

AWSTrustedAdvisorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 2 月 22 日 21:24 UTC
- 編集日時: 2024 年 6 月 11 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v13 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Sid" : "TrustedAdvisorServiceRolePermissions",
    "Effect" : "Allow",
    "Action" : [
      "access-analyzer:ListAnalyzers",
      "autoscaling:DescribeAccountLimits",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribeLaunchConfigurations",
      "ce:GetReservationPurchaseRecommendation",
      "ce:GetSavingsPlansPurchaseRecommendation",
      "cloudformation:DescribeAccountLimits",
      "cloudformation:DescribeStacks",
      "cloudformation:ListStacks",
      "cloudfront:ListDistributions",
      "cloudtrail:DescribeTrails",
      "cloudtrail:GetTrailStatus",
      "cloudtrail:GetTrail",
      "cloudtrail:ListTrails",
      "cloudtrail:GetEventSelectors",
      "cloudwatch:GetMetricStatistics",
      "cloudwatch:ListMetrics",
      "dax:DescribeClusters",
      "dynamodb:DescribeLimits",
      "dynamodb:DescribeTable",
      "dynamodb:ListTables",
      "ec2:DescribeAddresses",
      "ec2:DescribeReservedInstances",
      "ec2:DescribeInstances",
      "ec2:DescribeVpcs",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeImages",
      "ec2:DescribeNatGateways",
      "ec2:DescribeVolumes",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeRegions",
      "ec2:DescribeReservedInstancesOfferings",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeVpnGateways",
      "ec2:DescribeLaunchTemplateVersions",
```

```
"ec2:GetManagedPrefixListEntries",
"ecs:DescribeTaskDefinition",
"ecs:ListTaskDefinitions",
"elasticloadbalancing:DescribeAccountLimits",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeLoadBalancerAttributes",
"elasticloadbalancing:DescribeLoadBalancerPolicies",
"elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetServerCertificate",
"iam:ListServerCertificates",
"iam:ListSAMLProviders",
"kinesis:DescribeLimits",
"kafka:DescribeClusterV2",
"kafka:ListClustersV2",
"kafka:ListNodes",
"network-firewall:ListFirewalls",
"network-firewall:DescribeFirewall",
"outposts:ListAssets",
"outposts:GetOutpost",
"outposts:ListOutposts",
"rds:DescribeAccountAttributes",
"rds:DescribeDBClusters",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBParameters",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEngineDefaultParameters",
"rds:DescribeEvents",
"rds:DescribeOptionGroupOptions",
"rds:DescribeOptionGroups",
"rds:DescribeOrderableDBInstanceOptions",
"rds:DescribeReservedDBInstances",
"rds:DescribeReservedDBInstancesOfferings",
"rds:ListTagsForResource",
```

```
    "redshift:DescribeClusters",
    "redshift:DescribeReservedNodeOfferings",
    "redshift:DescribeReservedNodes",
    "route53:GetAccountLimit",
    "route53:GetHealthCheck",
    "route53:GetHostedZone",
    "route53:ListHealthChecks",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets",
    "route53resolver:ListResolverEndpoints",
    "route53resolver:ListResolverEndpointIpAddresses",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketVersioning",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetLifecycleConfiguration",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "ses:GetSendQuota",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSUserNotificationsServiceLinkedRolePolicy

説明：AWS ユーザー通知がユーザーに代わって AWS サービスを呼び出すことを許可します。

AWSUserNotificationsServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 19 日 13:28 UTC
- 編集日時: 2023 年 4 月 19 日 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSVendorInsightsAssessorFullAccess

説明： 権限を持つ Vendor Insights リソースを表示し、 Vendor Insights サブスクリプションを管理するためのフルアクセスを提供します

AWSVendorInsightsAssessorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsAssessorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSVendorInsightsAssessorReadOnly

説明： 権限を持つ Vendor Insights リソースを表示するための読み取り専用アクセスを提供します

AWSVendorInsightsAssessorReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsAssessorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSVendorInsightsVendorFullAccess

説明： Vendor Insights リソースを作成および管理するためのフルアクセスを提供します

AWSVendorInsightsVendorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2023 年 10 月 19 日 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSVendorInsightsVendorReadOnly

説明： Vendor Insights リソースを表示するための読み取り専用アクセスを提供します

AWSVendorInsightsVendorReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSVendorInsightsVendorReadOnly をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 7 月 26 日 15:05 UTC
- 編集日時: 2022 年 12 月 1 日 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSVpcLatticeServiceRolePolicy

説明： VPC Lattice がユーザーに代わって AWS リソースにアクセスできるようにします。

AWSVpcLatticeServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 30 日 20:47 UTC
- 編集日時: 2022 年 11 月 30 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSVPCS2SVpnServiceRolePolicy

説明： Site-to-Site VPN が VPN 接続に関連するリソースを作成および管理できるようにします。

AWSVPCS2SVpnServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 8 月 6 日 14:13 UTC
- 編集日時: 2019 年 8 月 6 日 14:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSVPCTransitGatewayServiceRolePolicy

説明： VPC Transit Gateway が Transit Gateway VPC アタッチメントに必要なリソースを作成および管理できるようにします。

AWSVPCTransitGatewayServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 26 日 16:21 UTC
- 編集日時: 2021 年 4 月 15 日 16:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSVPCVerifiedAccessServiceRolePolicy

説明： AWS Verified Access サービスがユーザーに代わってエンドポイントをプロビジョニングできるようにするポリシー

AWSVPCVerifiedAccessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 03:35 UTC
- 編集日時: 2023 年 11 月 17 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSWAFConsoleFullAccess

説明： 経由で AWS WAF へのフルアクセスを提供します AWS Management Console。このポリシーは、Amazon CloudFront デイストリビューションを一覧表示および更新するアクセス許可、

AWS Elastic Load Balancing でロードバランサーを表示するアクセス許可、Amazon API Gateway REST APIs およびステージを表示するアクセス許可、Amazon CloudWatch メトリクスを一覧表示および表示するアクセス許可、アカウント内で有効になっているリージョンを表示するアクセス許可も付与することに注意してください。

AWSWAFConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 6 日 18:38 UTC
- 編集日時: 2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSWAFConsoleReadOnlyAccess

説明： 経由で AWS WAF への読み取り専用アクセスを提供します AWS Management Console。このポリシーは、Amazon CloudFront デイストリビューションを一覧表示するアクセス許可、AWS Elastic Load Balancing でロードバランサーを表示するアクセス許可、Amazon API Gateway REST APIs とステージを表示するアクセス許可、Amazon CloudWatch メトリクスを一覧表示および表示

するアクセス許可、およびアカウント内で有効になっているリージョンを表示するアクセス許可も付与することに注意してください。

AWSWAFConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 6 日 18:43 UTC
- 編集日時: 2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSWAFFullAccess

説明 : AWS WAF アクションへのフルアクセスを提供します。

AWSWAFFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 6 日 20:44 UTC
- 編集日時: 2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSWAFReadOnlyAccess

説明： AWS WAF アクションへの読み取り専用アクセスを提供します。

AWSWAFReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWAFReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 10 月 6 日 20:43 UTC
- 編集日時: 2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

説明： が顧客に代わって リソースに関連する AWS サービスと WellArchitected リソースにアクセス WellArchitected できるようにします。

AWSWellArchitectedDiscoveryServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 4 月 26 日 18:36 UTC
- 編集日時: 2023 年 4 月 26 日 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
  ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

説明： Well-Architected がユーザーに代わって Organizations にアクセスできるようにします。

AWSWellArchitectedOrganizationsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 6 月 23 日 17:15 UTC
- 編集日時: 2022 年 7 月 25 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSWickrFullAccess

説明：このポリシーは、の Wickr 管理機能を含む、Wickr サービスへの完全な管理アクセス許可を付与します AWS Management Console。

AWSWickrFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSWickrFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 20:36 UTC

- 編集日時: 2022 年 11 月 27 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSXrayCrossAccountSharingConfiguration

説明: Observability Access Manager リンクを管理し、X-Ray トレースの共有を確立する機能を提供します。

AWSXrayCrossAccountSharingConfiguration は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `AWSXrayCrossAccountSharingConfiguration` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:46 UTC
- 編集日時: 2022 年 11 月 27 日 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSXRayDaemonWriteAccess

説明: AWS X-Ray デーモンが raw トレースセグメントデータをサービスの API に中継し、X-Ray SDK で使用するサンプリングデータ (ルール、ターゲットなど) を取得できるようにします。

AWSXRayDaemonWriteAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXRayDaemonWriteAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 8 月 28 日 23:00 UTC

- 編集日時 : 2024 年 2 月 13 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

AWSXrayFullAccess

説明： AWS X-Ray フルアクセス管理ポリシー

AWSXrayFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:30 UTC
- 編集日時: 2024 年 4 月 11 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSXrayReadOnlyAccess

説明： AWS X-Ray 読み取り専用マネージドポリシー

AWSXrayReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:27 UTC
- 編集日時: 2024 年 2 月 14 日 00:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSXrayWriteOnlyAccess

説明： AWS X-Ray 書き込み専用マネージドポリシー

AWSXrayWriteOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに AWSXrayWriteOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 1 日 18:19 UTC
- 編集日時: 2018 年 8 月 28 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

説明： ARC ゾーンシフト練習実行の管理アクセスと、練習実行をモニタリングするための CloudWatch アラームステータスへのアクセスを提供します。

AWSZonalAutoshiftPracticeRunSLRPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 29 日 17:34 UTC
- 編集日時: 2023 年 11 月 29 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

BatchServiceRolePolicy

説明： Amazon EC2 や Amazon ECS リソースなど、必要なリソースを管理するための AWS Batch サービスへのアクセスを提供します。

BatchServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 3 月 10 日 06:55 UTC
- 編集日時: 2023 年 12 月 5 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

Billing

説明: 請求とコスト管理のアクセス許可を付与します。これには、アカウントの使用状況の閲覧、ならびに予算および支払い方法の修正および閲覧が含まれます。

Billing は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに Billing をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:33 UTC
- 編集日時: 2024 年 5 月 23 日 23:26 UTC
- ARN: arn:aws:iam::aws:policy/job-function/Billing

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
```

```
"billing:GetIAMAccessPreference",
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"billing:PutContractInformation",
"billing:RedeemCredits",
"billing:UpdateBillingPreferences",
"billing:UpdateIAMAccessPreference",
"budgets:CreateBudgetAction",
"budgets>DeleteBudgetAction",
"budgets:DescribeBudgetActionsForBudget",
"budgets:DescribeBudgetAction",
"budgets:DescribeBudgetActionsForAccount",
"budgets:DescribeBudgetActionHistories",
"budgets:ExecuteBudgetAction",
"budgets:ModifyBudget",
"budgets:UpdateBudgetAction",
"budgets:ViewBudget",
"ce:CreateCostCategoryDefinition",
"ce:CreateNotificationSubscription",
"ce:CreateReport",
"ce>DeleteCostCategoryDefinition",
"ce>DeleteNotificationSubscription",
"ce>DeleteReport",
"ce:DescribeCostCategoryDefinition",
"ce:GetCostAndUsage",
"ce:ListCostAllocationTags",
"ce:ListCostCategoryDefinitions",
"ce:ListTagsForResource",
"ce:TagResource",
"ce:UpdateCostAllocationTagsStatus",
"ce:UpdateNotificationSubscription",
"ce:UpdatePreferences",
"ce:UpdateReport",
"ce:UpdateCostCategoryDefinition",
"ce:UntagResource",
"ce:StartCostAllocationTagBackfill",
"ce:ListCostAllocationTagBackfillHistory",
"ce:GetTags",
"ce:GetDimensionValues",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cur>DeleteReportDefinition",
"cur:DescribeReportDefinitions",
"cur:GetClassicReport",
```

```
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"cur:ModifyReportDefinition",
"cur:PutClassicReportPreferences",
"cur:PutReportDefinition",
"cur:ValidateReportDestination",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"freetier:PutFreeTierAlertPreference",
" invoicing:GetInvoiceEmailDeliveryPreferences",
" invoicing:GetInvoicePDF",
" invoicing>ListInvoiceSummaries",
" invoicing:PutInvoiceEmailDeliveryPreferences",
" payments>CreatePaymentInstrument",
" payments>DeletePaymentInstrument",
" payments:GetPaymentInstrument",
" payments:GetPaymentStatus",
" payments>ListPaymentPreferences",
" payments>ListTagsForResource",
" payments>ListPaymentInstruments",
" payments:MakePayment",
" payments:TagResource",
" payments:UpdatePaymentPreferences",
" payments:UpdatePaymentInstrument",
" payments:UntagResource",
" pricing:DescribeServices",
" purchase-orders:AddPurchaseOrder",
" purchase-orders>DeletePurchaseOrder",
" purchase-orders:GetPurchaseOrder",
" purchase-orders>ListPurchaseOrderInvoices",
" purchase-orders>ListPurchaseOrders",
" purchase-orders>ListTagsForResource",
" purchase-orders:ModifyPurchaseOrders",
" purchase-orders:TagResource",
" purchase-orders:UntagResource",
" purchase-orders:UpdatePurchaseOrder",
" purchase-orders:UpdatePurchaseOrderStatus",
" purchase-orders:ViewPurchaseOrders",
" support>CreateCase",
" support:AddAttachmentsToSet",
" sustainability:GetCarbonFootprintSummary",
" tax:BatchPutTaxRegistration",
" tax>DeleteTaxRegistration",
" tax:GetExemptions",
```



```
    "tax:GetTaxInheritance",
    "tax:GetTaxInterview",
    "tax:GetTaxRegistration",
    "tax:GetTaxRegistrationDocument",
    "tax:ListTaxRegistrations",
    "tax:PutTaxInheritance",
    "tax:PutTaxInterview",
    "tax:PutTaxRegistration",
    "tax:UpdateExemptions"
  ],
  "Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CertificateManagerServiceRolePolicy

説明 : Amazon Certificate Manager サービスロールポリシー

CertificateManagerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 6 月 25 日 17:56 UTC
- 編集日時: 2020 年 6 月 25 日 17:56 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ClientVPNServiceConnectionsRolePolicy

説明: AWS クライアント VPN がクライアント VPN エンドポイント接続を管理できるようにするポリシー。

ClientVPNServiceConnectionsRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 19:48 UTC
- 編集日時: 2020 年 8 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ClientVPNServiceRolePolicy

説明: AWS クライアント VPN がクライアント VPN エンドポイントを管理できるようにするポリシー。

ClientVPNServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 10 日 21:20 UTC
- 編集日時: 2020 年 8 月 12 日 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

ポリシーのバージョニング

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

説明 : CloudFormation StackSets (Organization Master Account) のサービスロール

CloudFormationStackSetsOrgAdminServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 10 日 00:20 UTC
- 編集日時: 2019 年 12 月 10 日 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

説明 : CloudFormation StackSets (組織メンバーアカウント) のサービスロール

CloudFormationStackSetsOrgMemberServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 9 日 23:52 UTC
- 編集日時: 2019 年 12 月 9 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudFrontFullAccess

説明： CloudFront コンソールへのフルアクセスと、 経由で Amazon S3 バケットを一覧表示する機能を提供します AWS Management Console。

CloudFrontFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudFrontFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2024 年 1 月 4 日 16:56 UTC
- ARN: arn:aws:iam::aws:policy/CloudFrontFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
```

```
    },
    {
      "Sid" : "cffullaccess",
      "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::*:*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudFrontReadOnlyAccess

説明： 経由でデイス CloudFront トリビューション設定情報とリストディストリビューションへのアクセスを提供します AWS Management Console。

CloudFrontReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudFrontReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2024 年 1 月 4 日 16:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudHSMServiceRolePolicy

説明： CloudHSM が使用または管理する AWS リソースへのアクセスを有効にする

CloudHSMServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 6 日 19:12 UTC

- 編集日時: 2017 年 11 月 6 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudSearchFullAccess

説明 : Amazon CloudSearch 設定サービスへのフルアクセスを提供します。

CloudSearchFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudSearchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudSearchReadOnlyAccess

説明： Amazon CloudSearch 設定サービスへの読み取り専用アクセスを提供します。

CloudSearchReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudSearchReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",

```

```
        "cloudsearch:List*"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudTrailServiceRolePolicy

説明： のアクセス許可ポリシー CloudTrail ServiceLinkedRole

CloudTrailServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 10 月 24 日 21:21 UTC
- 編集日時: 2023 年 11 月 27 日 01:18 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatch-CrossAccountAccess

説明 : CloudWatch が、クロスアカウント、クロスリージョンのデータを表示するために、現在のアカウントに代わってリモートアカウントの CloudWatchCrossAccountSharing ロールを引き受けることを許可します

CloudWatch-CrossAccountAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 7 月 23 日 09:59 UTC
- 編集日時: 2019 年 7 月 23 日 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchActionsEC2Access

説明： CloudWatch アラームとメトリクス、および EC2 メタデータへの読み取り専用アクセスを提供します。EC2 インスタンスを停止、終了、再起動するためのアクセスを提供します。

CloudWatchActionsEC2Access は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchActionsEC2Access をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 7 日 00:00 UTC
- 編集日時: 2015 年 7 月 7 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "cloudwatch:Describe*",
    "ec2:Describe*",
    "ec2:RebootInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : "*"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchAgentAdminPolicy

説明: を使用するために必要な完全なアクセス許可 AmazonCloudWatchAgent。

CloudWatchAgentAdminPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchAgentAdminPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 00:52 UTC
- 編集日時: 2024 年 2 月 5 日 20:59 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchAgentServerPolicy

説明： サーバー AmazonCloudWatchAgent で 使用するために必要なアクセス許可

CloudWatchAgentServerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchAgentServerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 3 月 7 日 01:06 UTC
- 編集日時: 2024 年 2 月 6 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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-*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchApplicationInsightsFullAccess

説明： CloudWatch Application Insights と必要な依存関係へのフルアクセスを提供します。

CloudWatchApplicationInsightsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchApplicationInsightsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 24 日 18:44 UTC
- 編集日時: 2022 年 1 月 25 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchApplicationInsightsReadOnlyAccess

説明： CloudWatch Application Insights への読み取り専用アクセスを提供します。

CloudWatchApplicationInsightsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchApplicationInsightsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 24 日 18:48 UTC
- 編集日時: 2020 年 11 月 24 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

説明： Cloudwatch Application Insights サービスにリンクされたロールポリシー

CloudwatchApplicationInsightsServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 12 月 1 日 16:22 UTC
- 編集日時: 2023 年 5 月 11 日 16:34 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v24 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchApplicationSignalsFullAccess

説明： CloudWatch Application Signals サービスへのフルアクセスと、このサービスの使用と運用に必要な依存関係へのスコープ付きアクセスを提供します。

CloudWatchApplicationSignalsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchApplicationSignalsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 6 日 22:50 UTC
- 編集日時: 2024 年 6 月 6 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    }
  ]
}
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
  ],
  {
```



```
"Sid" : "CloudWatchApplicationSignalsRumPermissions",
"Effect" : "Allow",
"Action" : [
  "rum:BatchCreateRumMetricDefinitions",
  "rum:BatchDeleteRumMetricDefinitions",
  "rum:BatchGetRumMetricDefinitions",
  "rum:GetAppMonitor",
  "rum:GetAppMonitorData",
  "rum:ListAppMonitors",
  "rum:PutRumMetricsDestination",
  "rum:UpdateRumMetricDefinition"
],
"Resource" : "*"
},
{
  "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
  "Effect" : "Allow",
  "Action" : "xray:GetTraceSummaries",
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
  "Effect" : "Allow",
  "Action" : "cloudwatch:PutMetricAlarm",
  "Resource" : [
    "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
    "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
    "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
  ]
},
{
  "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
  "Condition" : {
    "StringLike" : {
      "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
    }
  }
},
{
  "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
```

```
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
    "Effect" : "Allow",
    "Action" : [
      "sns:CreateTopic",
      "sns:Subscribe"
    ],
    "Resource" : "arn:aws:sns::*:cloudwatch-application-signals-*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
    "Effect" : "Allow",
    "Action" : "sns:ListTopics",
    "Resource" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchApplicationSignalsReadOnlyAccess

説明： CloudWatch Application Signals サービスへの読み取り専用アクセスと、このサービスの使用に必要な依存関係へのスコープ付きアクセスを提供します。

CloudWatchApplicationSignalsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `CloudWatchApplicationSignalsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 6 月 6 日 22:48 UTC
- 編集日時: 2024 年 6 月 6 日 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
  },
  {
    "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:GetRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:StartQuery"
    ],
    "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
    "Effect" : "Allow",
    "Action" : [
      "logs:StopQuery",
      "logs:GetQueryResults"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:DescribeAlarms"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData",
      "cloudwatch:ListMetrics"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "synthetics:DescribeCanaries",
  "synthetics:DescribeCanariesLastRun",
  "synthetics:GetCanaryRuns"
],
"Resource" : "*"
},
{
  "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
  "Effect" : "Allow",
  "Action" : [
    "rum:BatchGetRumMetricDefinitions",
    "rum:GetAppMonitor",
    "rum:GetAppMonitorData",
    "rum:ListAppMonitors"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
  "Effect" : "Allow",
  "Action" : [
    "xray:GetTraceSummaries"
  ],
  "Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchApplicationSignalsServiceRolePolicy

説明: ポリシーは、他の関連 AWS サービスからモニタリングおよびタグ付けデータを収集するアクセス許可を CloudWatch Application Signals に付与します。

CloudWatchApplicationSignalsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 9 日 18:09 UTC
- 編集日時: 2024 年 4 月 26 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "CWLogsPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "CWListMetricsPermission",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:ListMetrics"
    ],
    "Resource" : [
        "*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "CWGetMetricDataPermission",
```

```
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:GetMetricData"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Sid" : "TagsPermission",
    "Effect" : "Allow",
    "Action" : [
      "tag:GetResources"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid" : "EC2AutoScalingPermission",
    "Effect" : "Allow",
    "Action" : [
      "autoscaling:DescribeAutoScalingGroups"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
      }
    }
  }
]
```


詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchAutomaticDashboardsAccess

説明： Lambda 関数などのオブジェクトの内容を含む、CloudWatch 自動ダッシュボードの表示 CloudWatch APIs に使用される API 以外の へのアクセスを提供します

CloudWatchAutomaticDashboardsAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchAutomaticDashboardsAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 23 日 10:01 UTC
- 編集日時: 2021 年 4 月 20 日 13:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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*"  
]  
}  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchCrossAccountSharingConfiguration

説明： Observability Access Manager リンクを管理し、 CloudWatch リソースの共有を確立する機能を提供します。

CloudWatchCrossAccountSharingConfiguration は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 14:01 UTC
- 編集日時: 2022 年 11 月 27 日 14:01 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchEventsBuiltInTargetExecutionAccess

説明： Amazon CloudWatch Events の組み込みターゲットがユーザーに代わって EC2 アクションを実行できるようにします。

CloudWatchEventsBuiltInTargetExecutionAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsBuiltInTargetExecutionAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:35 UTC
- 編集日時: 2016 年 1 月 14 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchEventsFullAccess

説明： Amazon Events へのフルアクセス CloudWatch を提供します。

CloudWatchEventsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2016 年 1 月 14 日 18:37 UTC
- 編集日時: 2022 年 12 月 1 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchEventsInvocationAccess

説明： Amazon CloudWatch Events がアカウントの AWS Kinesis Streams のストリームにイベントを中継できるようにします。

CloudWatchEventsInvocationAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsInvocationAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2016 年 1 月 14 日 18:36 UTC
- 編集日時: 2016 年 1 月 14 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchEventsReadOnlyAccess

説明： Amazon Events への読み取り専用アクセス CloudWatch を提供します。

CloudWatchEventsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchEventsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 1 月 14 日 18:27 UTC
- 編集日時: 2022 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchEventsServiceRolePolicy

説明： アラームとイベントを使用して設定されたアクションを がユーザーに代わって実行 AWS CloudWatch できるようにします。

CloudWatchEventsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 17 日 00:42 UTC
- 編集日時: 2017 年 11 月 17 日 00:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchFullAccess

説明： へのフルアクセスを提供します CloudWatch。

CloudWatchFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2022 年 11 月 27 日 13:23 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchFullAccessV2

説明： へのフルアクセスを提供します CloudWatch。

CloudWatchFullAccessV2 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchFullAccessV2 をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 8 月 1 日 11:32 UTC
- 編集日時: 2024 年 5 月 17 日 22:20 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "CloudWatchFullAccessPermissions",
    "Effect" : "Allow",
    "Action" : [
      "application-autoscaling:DescribeScalingPolicies",
      "application-signals:*",
      "autoscaling:DescribeAutoScalingGroups",
      "autoscaling:DescribePolicies",
      "cloudwatch:*",
      "logs:*",
      "sns:CreateTopic",
      "sns:ListSubscriptions",
      "sns:ListSubscriptionsByTopic",
      "sns:ListTopics",
      "sns:Subscribe",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:GetRole",
      "oam:ListSinks",
      "rum:*",
      "synthetics:*",
      "xray:*"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "EventsServicePermissions",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "events.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "OAMReadPermissions",
    "Effect" : "Allow",
    "Action" : [
      "oam:ListAttachedLinks"
    ],
    "Resource" : "arn:aws:oam::*:sink/*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchInternetMonitorServiceRolePolicy

説明： Internet Monitor がユーザーに代わって EC2、Workspaces、 CloudFront リソース、 およびその他の必要なサービスにアクセスできるようにします。

CloudWatchInternetMonitorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 27 日 17:46 UTC
- 編集日時: 2023 年 7 月 20 日 04:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchLambdaInsightsExecutionRolePolicy

説明 : Lambda Insights Extension に必要なポリシー

CloudWatchLambdaInsightsExecutionRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLambdaInsightsExecutionRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 10 月 7 日 19:27 UTC

- 編集日時: 2020 年 10 月 7 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchLogsCrossAccountSharingConfiguration

説明： Observability Access Manager リンクを管理し、 CloudWatch Logs リソースの共有を確立する機能を提供します。

CloudWatchLogsCrossAccountSharingConfiguration は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLogsCrossAccountSharingConfiguration をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:55 UTC
- 編集日時: 2022 年 11 月 27 日 13:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchLogsFullAccess

説明： CloudWatch ログへのフルアクセスを提供します

CloudWatchLogsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLogsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 11 月 26 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchLogsReadOnlyAccess

説明： CloudWatch ログへの読み取り専用アクセスを提供します

CloudWatchLogsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchLogsReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2023 年 11 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchNetworkMonitorServiceRolePolicy

説明： CloudWatch Network Monitor が EC2 および VPC リソースにアクセスして管理し、ユーザーに代わってデータを発行 CloudWatch し、他の必要な サービスにアクセスできるようにします。

CloudWatchNetworkMonitorServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 12 月 21 日 18:53 UTC
- 編集日時: 2023 年 12 月 21 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CloudWatchReadOnlyAccess

説明： への読み取り専用アクセスを提供します CloudWatch。

CloudWatchReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2024 年 5 月 17 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",

```

```
    "synthetics:Get*",
    "synthetics:List*",
    "xray:BatchGet*",
    "xray:Get*"
  ],
  "Resource" : "*"
},
{
  "Sid" : "OAMReadPermissions",
  "Effect" : "Allow",
  "Action" : [
    "oam:ListAttachedLinks"
  ],
  "Resource" : "arn:aws:oam:*:*:sink/*"
},
{
  "Sid" : "CloudWatchReadOnlyGetRolePermissions",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchSyntheticsFullAccess

説明： CloudWatch Synthetics へのフルアクセスを提供します。

CloudWatchSyntheticsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchSyntheticsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 25 日 17:39 UTC
- 編集日時: 2022 年 5 月 6 日 18:14 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v9 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CloudWatchSyntheticsReadOnlyAccess

説明： CloudWatch Synthetics への読み取り専用アクセスを提供します。

CloudWatchSyntheticsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CloudWatchSyntheticsReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 11 月 25 日 17:45 UTC
- 編集日時: 2020 年 3 月 6 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "synthetics:Describe*",
      "synthetics:Get*",
      "synthetics:List*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ComprehendDataAccessRolePolicy

説明： データアクセスのための S3 リソースへのアクセスを許可する AWS Comprehend サービスロールのポリシー

ComprehendDataAccessRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ComprehendDataAccessRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2019 年 3 月 6 日 22:28 UTC
- 編集日時: 2019 年 3 月 6 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3::*Comprehend*",
      "arn:aws:s3::*comprehend*"
    ]
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ComprehendFullAccess

説明 : Amazon Comprehend へのフルアクセスを提供します。

ComprehendFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `ComprehendFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 18:08 UTC
- 編集日時: 2017 年 12 月 5 日 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ComprehendMedicalFullAccess

説明： Amazon Comprehend Medical へのフルアクセスを提供します

ComprehendMedicalFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ComprehendMedicalFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 17:55 UTC
- 編集日時: 2018 年 11 月 27 日 17:55 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendMedicalFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```



```
{
  "Action" : [
    "comprehendmedical:*"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ComprehendReadOnly

説明： Amazon Comprehend への読み取り専用アクセスを提供します。

ComprehendReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ComprehendReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 18:10 UTC
- 編集日時: 2022 年 4 月 26 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendReadOnly

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ComputeOptimizerReadOnlyAccess

説明： への読み取り専用アクセスを提供します ComputeOptimizer。

ComputeOptimizerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ComputeOptimizerReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 3 月 7 日 00:11 UTC
- 編集日時: 2023 年 8 月 28 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ComputeOptimizerServiceRolePolicy

説明： ComputeOptimizer がユーザーに代わって AWS サービスを呼び出し、ワークロードの詳細を収集できるようにします。

ComputeOptimizerServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 3 日 08:45 UTC
- 編集日時: 2022 年 6 月 13 日 19:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ConfigConformsServiceRolePolicy

説明: がコンフォーマンスパックを作成 AWSConfig するために必要なポリシー

ConfigConformsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 7 月 25 日 21:38 UTC
- 編集日時: 2023 年 1 月 12 日 04:17 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CostOptimizationHubAdminAccess

説明： この管理ポリシーは、Cost Optimization Hub への管理者アクセスを提供します。

CostOptimizationHubAdminAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CostOptimizationHubAdminAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 19 日 00:03 UTC
- 編集日時: 2023 年 12 月 19 日 00:03 UTC
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        ]
      }
    }
  }
]
```

```
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

CostOptimizationHubReadOnlyAccess

説明： この管理ポリシーは、Cost Optimization Hub への読み取り専用アクセスを提供します。

CostOptimizationHubReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに CostOptimizationHubReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 13 日 18:04 UTC
- 編集日時: 2023 年 12 月 13 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CostOptimizationHubServiceRolePolicy

説明： Cost Optimization Hub が組織情報を取得し、最適化関連のデータとメタデータを収集できるようにします。

CostOptimizationHubServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 11 月 26 日 08:03 UTC
- 編集日時: 2023 年 11 月 26 日 08:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
        "*"
    ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

CustomerProfilesServiceLinkedRolePolicy

説明 : Amazon Connect Customer Profiles がユーザーに代わって AWS サービスとリソースにアクセスできるようにします。

CustomerProfilesServiceLinkedRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 3 月 7 日 22:56 UTC
- 編集日時: 2023 年 3 月 7 日 22:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

DatabaseAdministrator

説明： AWS データベース AWS サービスの設定と設定に必要な サービスとアクションへのフルアクセス許可を付与します。

DatabaseAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに DatabaseAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:25 UTC
- 編集日時: 2019 年 1 月 8 日 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

DataScientist

説明: AWS データ分析サービスにアクセス許可を付与します。

DataScientist は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに DataScientist をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:28 UTC
- 編集日時: 2019 年 12 月 3 日 16:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

DAXServiceRolePolicy

説明：このポリシーは、DAX がお客様に代わってネットワークインターフェイス、セキュリティグループ、サブネット、および Vpc を作成および管理することを許可します。

DAXServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 5 日 17:51 UTC
- 編集日時: 2018 年 3 月 5 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"   
}   
]   
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

説明： Amazon DynamoDB の Amazon CloudWatch Contributor Insights をサポートするために必要なアクセス許可。

DynamoDBCloudWatchContributorInsightsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 15 日 21:13 UTC
- 編集日時: 2019 年 11 月 15 日 21:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

DynamoDBKinesisReplicationServiceRolePolicy

説明 : AWS DynamoDB に へのアクセスを提供する KinesisDataStreams

DynamoDBKinesisReplicationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 12 日 00:43 UTC
- 編集日時: 2020 年 11 月 12 日 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

DynamoDBReplicationServiceRolePolicy

説明： DynamoDB がクロスリージョンデータレプリケーションに必要なアクセス許可

DynamoDBReplicationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 11 月 9 日 23:55 UTC
- 編集日時: 2024 年 1 月 8 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

EC2FastLaunchFullAccess

説明： このポリシーは、EC2 Fast Launch アクションへのフルアクセスを付与します

EC2FastLaunchFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2FastLaunchFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2024 年 5 月 13 日 22:45 UTC
- 編集日時: 2024 年 5 月 13 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:image/*",

```

```
    "arn:aws:ec2:*:*:key-pair/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ]
},
{
  "Sid" : "EC2LaunchInstanceWithVolAndInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
    }
  }
},
{
  "Sid" : "EC2Tags",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:vpc/*",
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "RunInstances"
    }
  }
},
{
  "Sid" : "IAMSLR",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
```

```
    "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "IAMSLRPassRole",
    "Effect" : "Allow",
    "Action" : "iam:PassRole",
    "Resource" : [
      "arn:aws:iam::*:instance-profile/*",
      "arn:aws:iam::*:role/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com",
          "ec2.amazonaws.com.cn"
        ]
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

EC2FastLaunchServiceRolePolicy

説明：ポリシーは、お客様のアカウントで事前プロビジョニングされたスナップショットを準備および管理し、関連メトリクスを発行するための ec2fastlaunch を付与します。

EC2FastLaunchServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 1 月 10 日 13:08 UTC
- 編集日時: 2022 年 1 月 10 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
    "arn:aws:ec2:*:*:launch-template/*"
  ],
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : "iam:PassRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com",
        "ec2.amazonaws.com.cn"
      ]
    }
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshot",
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  },
  {
    "Sid" : "AllowCreateTaggedSnapshot",
    "Effect" : "Allow",
    "Action" : "ec2:CreateSnapshot",
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
      },
      "StringLike" : {
        "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
      },
      "ForAnyValue:StringEquals" : {
        "aws:TagKeys" : [
          "CreatedByLaunchTemplateName",
          "CreatedByLaunchTemplateId"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateLaunchTemplate",
    "Resource" : "arn:aws:ec2:*:*:launch-template/*",
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  }
}
```

```
    }
  },
  {
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : [
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:launch-template/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "CreateSnapshot",
          "RunInstances",
          "CreateLaunchTemplate"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteSnapshot"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
```

```
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates"
    ],
    "Resource" : "*"
},
{
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "cloudwatch:namespace" : "AWS/EC2"
        }
    }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

EC2FleetTimeShiftableServiceRolePolicy

説明: EC2 フリートに将来インスタンスを起動するためのアクセス許可を付与するポリシー。

EC2FleetTimeShiftableServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 23 日 19:47 UTC

- 編集日時: 2019 年 12 月 23 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
        }
    }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

Ec2ImageBuilderCrossAccountDistributionAccess

説明： EC2 Image Builder がクロスアカウントディストリビューションを実行するために必要なアクセス許可。

Ec2ImageBuilderCrossAccountDistributionAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに Ec2ImageBuilderCrossAccountDistributionAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 30 日 19:22 UTC
- 編集日時: 2020 年 9 月 30 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/
Ec2ImageBuilderCrossAccountDistributionAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

EC2ImageBuilderLifecycleExecutionPolicy

説明 : EC2ImageBuilderLifecycleExecutionPolicy ポリシーは、Image Builder に Image Builder イメージリソースとその基盤となるリソース (AMIs、スナップショット) を非推奨または削除するなどのアクションを実行するアクセス許可を付与し、イメージライフサイクル管理タスクの自動ルールをサポートします。

EC2ImageBuilderLifecycleExecutionPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2ImageBuilderLifecycleExecutionPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 11 月 16 日 23:23 UTC
- 編集日時: 2023 年 11 月 16 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
```

```
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*::snapshot/*",
    "arn:aws:ec2:*::image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
      "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : "DeprecatedBy"
    }
  }
},
{
  "Sid" : "ECRImagePermission",
  "Effect" : "Allow",
  "Action" : [
    "ecr:BatchGetImage",
    "ecr:BatchDeleteImage"
  ],
  "Resource" : "arn:aws:ecr:*::repository/*",
  "Condition" : {
    "StringEquals" : {
      "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
    }
  }
},
{
  "Sid" : "ImageBuilderEC2TagServicePermission",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeImages",
    "tag:GetResources",
    "imagebuilder>DeleteImage"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

EC2InstanceConnect

説明: 顧客が EC2 Instance Connect を呼び出して EC2 インスタンスにエフェメラルキーを発行し、ssh または EC2 Instance Connect CLI 経由で接続できるようにします。

EC2InstanceConnect は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2InstanceConnect をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 27 日 18:53 UTC
- 編集日時: 2019 年 6 月 27 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceConnect

ポリシーのバージョニング

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Sid" : "EC2InstanceConnect",
    "Action" : [
      "ec2:DescribeInstances",
      "ec2-instance-connect:SendSSHPublicKey"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

Ec2InstanceConnectEndpoint

説明：お客様が作成した EC2 Instance Connect エンドポイントを管理するための EC2 Instance Connect エンドポイントポリシー

Ec2InstanceConnectEndpoint は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 24 日 20:19 UTC
- 編集日時: 2023 年 1 月 24 日 20:19 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
      ]
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

EC2InstanceProfileForImageBuilder

説明 : Image Builder サービスの EC2 インスタンスプロファイル。

EC2InstanceProfileForImageBuilder は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに EC2InstanceProfileForImageBuilder をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 1 日 19:08 UTC
- 編集日時: 2020 年 8 月 27 日 16:40 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

説明： EC2 Image Builder でコンテナイメージを構築するための EC2 インスタンスプロファイル。このポリシーは、ユーザーが ECR イメージをアップロードするために広範な許可を付与します。

EC2InstanceProfileForImageBuilderECRContainerBuilds は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

EC2InstanceProfileForImageBuilderECRContainerBuilds をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 12 月 11 日 19:48 UTC
- 編集日時: 2020 年 12 月 11 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/
EC2InstanceProfileForImageBuilderECRContainerBuilds

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ECRReplicationServiceRolePolicy

説明: ECR レプリケーションによって使用または管理される AWS のサービス およびリソースへのアクセスを有効にする

ECRReplicationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 4 日 22:11 UTC
- 編集日時: 2020 年 12 月 4 日 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ElastiCacheServiceRolePolicy

説明: このポリシーでは ElastiCache、キャッシュを管理するために必要な AWS リソースを ユーザーに代わって管理することを許可します。

ElastiCacheServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 12 月 7 日 17:50 UTC
- 編集日時: 2023 年 11 月 28 日 03:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
```

```
    "ec2:CreateNetworkInterface",
    "ec2:CreateSecurityGroup",
    "ec2>DeleteNetworkInterface",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:RevokeSecurityGroupIngress",
    "cloudwatch:PutMetricData",
    "outposts:GetOutpost",
    "outposts:GetOutpostInstanceTypes",
    "outposts:ListOutposts",
    "outposts:ListSites"
  ],
  "Resource" : "*"
},
{
  "Sid" : "CreateDeleteVPCEndpoints",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringLike" : {
      "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
    }
  }
},
{
  "Sid" : "TagVPCEndpointsOnCreation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint",

```

```
        "aws:RequestTag/AmazonElastiCacheManaged" : "true"
    }
}
},
{
    "Sid" : "ModifyVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
    }
},
{
    "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElasticLoadBalancingFullAccess

説明： Amazon へのフルアクセスと ElasticLoadBalancing、 ElasticLoadBalancing 機能の提供に必要な他の サービスへの制限付きアクセスを提供します。

ElasticLoadBalancingFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElasticLoadBalancingFullAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 9 月 20 日 20:42 UTC
- 編集日時: 2022 年 11 月 29 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElasticLoadBalancingReadOnly

説明： Amazon ElasticLoadBalancing および依存サービスへの読み取り専用アクセスを提供します
ElasticLoadBalancingReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElasticLoadBalancingReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 9 月 20 日 20:17 UTC
- 編集日時: 2023 年 11 月 26 日 18:15 UTC
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ElementalActivationsDownloadSoftwareAccess

説明： 購入済みアセットの表示、関連ソフトウェアとキックスタートファイルのダウンロードへのアクセス

ElementalActivationsDownloadSoftwareAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsDownloadSoftwareAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 9 月 8 日 17:26 UTC
- 編集日時: 2020 年 9 月 8 日 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElementalActivationsFullAccess

説明： Elemental Appliances and Software が購入したアセットを表示してアクションを実行するためのフルアクセス

ElementalActivationsFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalActivationsFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 6 月 4 日 21:00 UTC
- 編集日時: 2020 年 6 月 4 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "elemental-activations:*"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ElementalActivationsGenerateLicenses

説明： 購入済みアセットを表示し、保留中のアクティベーションのソフトウェアライセンスを生成するアクセス

ElementalActivationsGenerateLicenses は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalActivationsGenerateLicenses をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 28 日 18:28 UTC
- 編集日時: 2020 年 8 月 28 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ElementalActivationsReadOnlyAccess

説明：AWS アカウント ユーザーのに関連付けられている購入済みアセットの詳細なリストへの読み取り専用アクセス

ElementalActivationsReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `ElementalActivationsReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 8 月 28 日 16:51 UTC
- 編集日時: 2020 年 8 月 28 日 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElementalAppliancesSoftwareFullAccess

説明： Elemental Appliances and Software の見積りと注文を表示してアクションを実行するためのフルアクセス

ElementalAppliancesSoftwareFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalAppliancesSoftwareFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 7 月 31 日 16:28 UTC
- 編集日時: 2021 年 2 月 5 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "elemental-appliances-software:*",
      "elemental-activations:CompleteAccountRegistration"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElementalAppliancesSoftwareReadOnlyAccess

説明 : Elemental Appliances and Software の見積りと注文を表示するための読み取り専用アクセス

ElementalAppliancesSoftwareReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalAppliancesSoftwareReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 1 日 22:31 UTC
- 編集日時: 2020 年 4 月 1 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ElementalSupportCenterFullAccess

説明： Elemental Appliance and Software サポートケースと製品サポートコンテンツを表示してアクションを実行するためのフルアクセス

ElementalSupportCenterFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ElementalSupportCenterFullAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 11 月 25 日 18:08 UTC
- 編集日時: 2021 年 2 月 5 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

EMRDescribeClusterPolicyForEMRWAL

説明: このポリシーは、Amazon EMR の WAL サービスがクラスターのステータスを検索して返すことを許可する読み取り専用アクセス許可を付与します。

EMRDescribeClusterPolicyForEMRWAL は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 6 月 15 日 23:30 UTC
- 編集日時: 2023 年 6 月 15 日 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "elasticmapreduce:DescribeCluster"
    ],
    "Resource" : "*"
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

FMSServiceRolePolicy

説明 : FM サービスにリンクされたロールが、お客様の AWS Organization アカウント内の FM マネージドリソースに対して FM 関連のアクションを実行することを許可するアクセスポリシー。

FMSServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 3 月 28 日 23:01 UTC
- 編集日時: 2024 年 4 月 22 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v29 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*:*/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
```

```
"Effect" : "Allow",
"Action" : [
  "wafv2:PutLoggingConfiguration",
  "wafv2:GetLoggingConfiguration",
  "wafv2:ListLoggingConfigurations",
  "wafv2>DeleteLoggingConfiguration"
],
"Resource" : [
  "arn:aws:wafv2:*:*:regional/webacl/*",
  "arn:aws:wafv2:*:*:global/webacl/*"
]
},
{
  "Sid" : "WafWebaclCreation",
  "Effect" : "Allow",
  "Action" : [
    "waf:CreateWebACL",
    "waf-regional:CreateWebACL",
    "waf:GetChangeToken",
    "waf-regional:GetChangeToken",
    "waf-regional:GetWebACLForResource"
  ],
  "Resource" : [
    "arn:aws:waf:*:*:*",
    "arn:aws:waf-regional:*:*:*"
  ]
},
{
  "Sid" : "ElbGeneral",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
    "elasticloadbalancing:DescribeTags"
  ],
  "Resource" : "*"
},
{
  "Sid" : "WafPermissionPolicy",
  "Effect" : "Allow",
  "Action" : [
    "waf:PutPermissionPolicy",
    "waf:GetPermissionPolicy",
    "waf>DeletePermissionPolicy",
    "waf-regional:PutPermissionPolicy",
```

```
    "waf-regional:GetPermissionPolicy",
    "waf-regional:DeletePermissionPolicy"
  ],
  "Resource" : [
    "arn:aws:waf:*:*:webacl/*",
    "arn:aws:waf:*:*:rulegroup/*",
    "arn:aws:waf-regional:*:*:webacl/*",
    "arn:aws:waf-regional:*:*:rulegroup/*"
  ]
},
{
  "Sid" : "CloudfrontGeneral",
  "Effect" : "Allow",
  "Action" : [
    "cloudfront:GetDistribution",
    "cloudfront:UpdateDistribution",
    "cloudfront:ListDistributionsByWebACLId",
    "cloudfront:ListDistributions",
    "cloudfront:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ConfigScoped",
  "Effect" : "Allow",
  "Action" : [
    "config>DeleteConfigRule",
    "config:GetComplianceDetailsByConfigRule",
    "config:PutConfigRule",
    "config:StartConfigRulesEvaluation",
    "config>DeleteEvaluationResults"
  ],
  "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/"
*
},
{
  "Sid" : "ConfigUnscoped",
  "Effect" : "Allow",
  "Action" : [
    "config:DescribeComplianceByConfigRule",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus",
    "config:DescribeConfigRules",
    "config:DescribeConfigRuleEvaluationStatus",
```

```
    "config:PutConfigurationRecorder",
    "config:StartConfigurationRecorder",
    "config:PutDeliveryChannel",
    "config:DescribeDeliveryChannels",
    "config:DescribeDeliveryChannelStatus",
    "config:GetComplianceSummaryByConfigRule",
    "config:GetDiscoveredResourceCounts",
    "config:PutEvaluations",
    "config>SelectResourceConfig"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SlrDeletion",
  "Effect" : "Allow",
  "Action" : [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource" : [
    "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
  ]
},
{
  "Sid" : "OrganizationsGeneral",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListChildren",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "ShieldGeneral",
  "Effect" : "Allow",
```

```
"Action" : [
  "shield:CreateProtection",
  "shield>DeleteProtection",
  "shield:DescribeProtection",
  "shield>ListProtections",
  "shield>ListAttacks",
  "shield>CreateSubscription",
  "shield:DescribeSubscription",
  "shield:GetSubscriptionState",
  "shield:DescribeDRTAccess",
  "shield:DescribeEmergencyContactSettings",
  "shield:UpdateEmergencyContactSettings",
  "elasticloadbalancing:DescribeLoadBalancers",
  "ec2:DescribeAddresses",
  "shield:EnableApplicationLayerAutomaticResponse",
  "shield:DisableApplicationLayerAutomaticResponse",
  "shield:UpdateApplicationLayerAutomaticResponse"
],
"Resource" : "*"
},
{
  "Sid" : "EC2SecurityGroupScoped",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2>DeleteSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
    "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Sid" : "SecurityGroupTagCreation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ]
},
```

```
"Resource" : [
  "arn:aws:ec2:*:*:security-group/*"
],
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : "CreateSecurityGroup"
  }
}
},
{
  "Sid" : "SecurityGroupTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteTags",
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/FMManaged" : "*"
    }
  }
}
},
{
  "Sid" : "Ec2Unscoped",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup",
    "ec2:DescribeSecurityGroupReferences",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeStaleSecurityGroups",
    "ec2:DescribeNetworkInterfaces",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeNetworkInterfaceAttribute",
    "ec2:DescribeInstances",
    "ec2:AssociateRouteTable",
    "ec2:CreateSubnet",
    "ec2:CreateRouteTable",
    "ec2>DeleteSubnet",
    "ec2:DisassociateRouteTable",
```



```
    "ec2:ReplaceRouteTableAssociation"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "Wafv2General",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:TagResource",
    "wafv2:ListResourcesForWebACL",
    "wafv2:AssociateWebACL",
    "wafv2:ListTagsForResource",
    "wafv2:UntagResource",
    "wafv2:GetWebACL",
    "wafv2:DisassociateFirewallManager",
    "wafv2>DeleteWebACL",
    "wafv2:DisassociateWebACL"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/webacl/*",
    "arn:aws:wafv2:*:*:regional/webacl/*"
  ]
},
{
  "Sid" : "Wafv2WebAclAndRuleGroupMutation",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:UpdateWebACL",
    "wafv2:CreateWebACL",
    "wafv2>DeleteFirewallManagerRuleGroups",
    "wafv2:PutFirewallManagerRuleGroups"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/webacl/*",
    "arn:aws:wafv2:*:*:regional/webacl/*",
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*",
    "arn:aws:wafv2:*:*:global/managedruleset/*",
    "arn:aws:wafv2:*:*:regional/managedruleset/*",
    "arn:aws:wafv2:*:*:global/ipset/*",
    "arn:aws:wafv2:*:*:regional/ipset/*",
    "arn:aws:wafv2:*:*:global/regexpatternset/*",
```

```
    "arn:aws:wafv2:*:*:regional/regexpatternset/*"
  ],
},
{
  "Sid" : "Wafv2PermissionPolicy",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:PutPermissionPolicy",
    "wafv2:GetPermissionPolicy",
    "wafv2>DeletePermissionPolicy"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:global/rulegroup/*",
    "arn:aws:wafv2:*:*:regional/rulegroup/*"
  ]
},
{
  "Sid" : "Wafv2WebaclDescribe",
  "Effect" : "Allow",
  "Action" : [
    "wafv2:GetWebACLForResource"
  ],
  "Resource" : [
    "arn:aws:wafv2:*:*:regional/webacl/*"
  ]
},
{
  "Sid" : "RouteTableTagManagement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateRouteTable"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
```

```
"Sid" : "SubnetTagManagement",
"Effect" : "Allow",
"Action" : "ec2:CreateTags",
"Resource" : [
  "arn:aws:ec2:*:*:subnet/*"
],
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  }
},
{
  "Sid" : "VPCEndpointTagManagement",
  "Effect" : "Allow",
  "Action" : "ec2:CreateTags",
  "Resource" : [
    "arn:aws:ec2:*:*:vpc-endpoint/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : "CreateVpcEndpoint"
    },
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Sid" : "RouteTableCleanup",
  "Effect" : "Allow",
  "Action" : "ec2:DeleteRouteTable",
  "Resource" : "arn:aws:ec2:*:*:route-table/*",
  "Condition" : {
    "StringEquals" : {
      "ec2:ResourceTag/FMManaged" : "true"
    }
  }
}
```

```
  },
  {
    "Sid" : "Ec2DescribeUnscoped",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DescribeInternetGateways",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSubnets",
      "ec2:DescribeTags",
      "ec2:DescribeVpcEndpoints",
      "ec2:DescribeAvailabilityZones"
    ],
    "Resource" : "*"
  },
  {
    "Sid" : "CreateVpcEndpointScoped",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:vpc-endpoint/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/FMManaged" : [
          "true"
        ]
      }
    }
  },
  {
    "Sid" : "CreateVpcEndpointUnscoped",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVpcEndpoint",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:vpc/*"
    ]
  },
  {
    "Sid" : "VpcEndpointsDeletion",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteVpcEndpoints"
    ]
  },
  ],
```

```
"Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
"Condition" : {
  "StringEquals" : {
    "ec2:ResourceTag/FMManaged" : "true"
  }
},
{
  "Sid" : "RamTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "ram:TagResource"
  ],
  "Resource" : [
    "arn:aws:ram:*:*:resource-share/*"
  ],
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Sid" : "RamMutation",
  "Effect" : "Allow",
  "Action" : [
    "ram:AssociateResourceShare",
    "ram:UpdateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource" : "arn:aws:ram:*:*:resource-share/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Sid" : "RamCreation",
  "Effect" : "Allow",
  "Action" : "ram:CreateResourceShare",
```

```
"Resource" : "*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged"
    ]
  },
  "StringEquals" : {
    "aws:RequestTag/FMManaged" : [
      "true"
    ]
  }
},
{
  "Sid" : "RamDescribe",
  "Effect" : "Allow",
  "Action" : [
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares"
  ],
  "Resource" : "*"
},
{
  "Sid" : "SlrCreation",
  "Effect" : "Allow",
  "Action" : "iam:CreateServiceLinkedRole",
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "iam:AWSServiceName" : [
        "network-firewall.amazonaws.com",
        "shield.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "IamDescribe",
  "Effect" : "Allow",
  "Action" : "iam:GetRole",
  "Resource" : "*"
},
```

```
{
  "Sid" : "NetworkFirewallTagManagement",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:TagResource"
  ],
  "Resource" : "*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged"
      ]
    }
  }
},
{
  "Sid" : "NetworkFirewallGeneral",
  "Effect" : "Allow",
  "Action" : [
    "network-firewall:AssociateSubnets",
    "network-firewall:CreateFirewall",
    "network-firewall:CreateFirewallPolicy",
    "network-firewall:DisassociateSubnets",
    "network-firewall:UpdateFirewallDeleteProtection",
    "network-firewall:UpdateFirewallPolicy",
    "network-firewall:UpdateFirewallPolicyChangeProtection",
    "network-firewall:UpdateSubnetChangeProtection",
    "network-firewall:AssociateFirewallPolicy",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall>ListFirewallPolicies",
    "network-firewall>ListFirewalls",
    "network-firewall>ListRuleGroups",
    "network-firewall:PutResourcePolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall>DeleteResourcePolicy",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:UpdateLoggingConfiguration"
  ],
  "Resource" : "*"
},
{
```

```
"Sid" : "NetworkFirewallCleanup",
"Effect" : "Allow",
"Action" : [
  "network-firewall:DeleteFirewallPolicy",
  "network-firewall:DeleteFirewall"
],
"Resource" : "*",
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/FMManaged" : "true"
  }
}
},
{
  "Sid" : "LogsGeneral",
  "Effect" : "Allow",
  "Action" : [
    "logs:ListLogDeliveries",
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs:DeleteLogDelivery"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Route53ResolverRuleGroupUnscoped",
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:ListFirewallRuleGroupAssociations",
    "route53resolver:ListTagsForResource",
    "route53resolver:ListFirewallRuleGroups",
    "route53resolver:GetFirewallRuleGroupAssociation",
    "route53resolver:GetFirewallRuleGroup",
    "route53resolver:GetFirewallRuleGroupPolicy",
    "route53resolver:PutFirewallRuleGroupPolicy"
  ],
  "Resource" : "*"
},
{
  "Sid" : "Route53ResolverRuleGroupCleanup",
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:UpdateFirewallRuleGroupAssociation",
```



```
    "route53resolver:DisassociateFirewallRuleGroup"
  ],
  "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
},
{
  "Sid" : "Route53ResolverRuleGroupScoped",
  "Effect" : "Allow",
  "Action" : [
    "route53resolver:AssociateFirewallRuleGroup",
    "route53resolver:TagResource"
  ],
  "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/FMManaged" : "true"
    }
  }
},
{
  "Sid" : "NaclTagCreation",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : "arn:aws:ec2:*:*:network-acl/*",
  "Condition" : {
    "ForAllValues:StringEquals" : {
      "aws:TagKeys" : [
        "Name",
        "FMManaged",
        "FMPolicies"
      ]
    },
    "StringEquals" : {
      "ec2:CreateAction" : "CreateNetworkAcl"
    }
  }
},
{
```

```
"Sid" : "NaclTagManagement",
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Resource" : "arn:aws:ec2:*:*:network-acl/*",
"Condition" : {
  "ForAllValues:StringEquals" : {
    "aws:TagKeys" : [
      "Name",
      "FMManaged",
      "FMPolicies"
    ]
  },
  "StringEquals" : {
    "aws:ResourceTag/FMManaged" : "true"
  }
}
},
{
  "Sid" : "NaclScoped",
  "Effect" : "Allow",
  "Action" : [
    "ec2>DeleteNetworkAclEntry",
    "ec2>CreateNetworkAclEntry",
    "ec2:ReplaceNetworkAclEntry",
    "ec2>DeleteNetworkAcl"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/FMManaged" : "true"
    }
  }
}
},
{
  "Sid" : "NaclUnscoped",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ReplaceNetworkAclAssociation",
    "ec2:DescribeNetworkAcls",
    "ec2>CreateNetworkAcl"
  ],
}
```

```
    "Resource" : "*"
  }
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

FSxDeleteServiceLinkedRoleAccess

説明 : Amazon FSx が Amazon S3 アクセスのサービスにリンクされたロールを削除することを許可する

FSxDeleteServiceLinkedRoleAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 28 日 10:40 UTC
- 編集日時: 2018 年 11 月 28 日 10:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

GameLiftGameServerGroupPolicy

説明: Gamelift がカスタマーリソース GameServerGroups を管理できるようにするポリシー

GameLiftGameServerGroupPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに GameLiftGameServerGroupPolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 4 月 3 日 23:12 UTC
- 編集日時: 2020 年 5 月 13 日 17:27 UTC

- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

GlobalAcceleratorFullAccess

説明： GlobalAccelerator ユーザーにすべての APIs

GlobalAcceleratorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに GlobalAcceleratorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 02:44 UTC
- 編集日時: 2020 年 12 月 4 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

GlobalAcceleratorReadOnlyAccess

説明：読み取り専用 API へのアクセスを GlobalAccelerator ユーザーに許可する APIs

GlobalAcceleratorReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `GlobalAcceleratorReadOnlyAccess` をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 02:41 UTC
- 編集日時: 2018 年 11 月 27 日 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

GreengrassOTAUpdateArtifactAccess

説明：すべての Greengrass リージョンで Greengrass OTA 更新アーティファクトへの読み取りアクセスを提供します

GreengrassOTAUpdateArtifactAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに GreengrassOTAUpdateArtifactAccess をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 11 月 29 日 18:11 UTC
- 編集日時: 2018 年 12 月 18 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*-greengrass-updates/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

GroundTruthSyntheticConsoleFullAccess

説明：このポリシーは、SageMaker Ground Truth 合成コンソールのすべての機能を使用するために必要なアクセス許可を付与します。

GroundTruthSyntheticConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに GroundTruthSyntheticConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC

- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

GroundTruthSyntheticConsoleReadOnlyAccess

説明: このポリシーは、経由で SageMaker Ground Truth Synthetic への読み取り専用アクセスを許可します AWS Management Console。

GroundTruthSyntheticConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに GroundTruthSyntheticConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 8 月 25 日 15:58 UTC
- 編集日時: 2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

Health_OrganizationsServiceRolePolicy

説明：組織ビュー機能を有効にする AWS ヘルスポリシー

Health_OrganizationsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 12 月 16 日 13:28 UTC
- 編集日時: 2024 年 2 月 6 日 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

IAMAccessAdvisorReadOnly

説明: このポリシーは、サービスの最終アクセス情報など、IAM アクセスアドバイザーによって提供されるすべてのアクセス情報を読み取るためのアクセスを許可します。

IAMAccessAdvisorReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMAccessAdvisorReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 21 日 19:33 UTC

- 編集日時: 2019 年 6 月 21 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

IAMAccessAnalyzerFullAccess

説明 : IAM Access Analyzer へのフルアクセスを提供します

IAMAccessAnalyzerFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMAccessAnalyzerFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集日時: 2019 年 12 月 2 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

IAMAccessAnalyzerReadOnlyAccess

説明： IAM Access Analyzer リソースへの読み取り専用アクセスを提供します

IAMAccessAnalyzerReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMAccessAnalyzerReadOnlyAccess をアタッチできません。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 12 月 2 日 17:12 UTC
- 編集日時: 2023 年 11 月 27 日 02:24 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IAMFullAccess

説明： 経由で IAM へのフルアクセスを提供します AWS Management Console。

IAMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2019 年 6 月 21 日 19:40 UTC

- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IAMReadOnlyAccess

説明： 経由で IAM への読み取り専用アクセスを提供します AWS Management Console。

IAMReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:40 UTC
- 編集日時: 2018 年 1 月 25 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",

```

```
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IAMSelfManageServiceSpecificCredentials

説明： IAM ユーザーが独自のサービス固有の認証情報を管理できるようにします。

IAMSelfManageServiceSpecificCredentials は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMSelfManageServiceSpecificCredentials をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 12 月 22 日 17:25 UTC
- 編集日時: 2016 年 12 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IAMUserChangePassword

説明： IAM ユーザーが自分のパスワードを変更できるようにします。

IAMUserChangePassword は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMUserChangePassword をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 11 月 15 日 00:25 UTC
- 編集日時: 2016 年 11 月 15 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IAMUserSSHKeys

説明： IAM ユーザーが独自の SSH キーを管理できるようにします。

IAMUserSSHKeys は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IAMUserSSHKeys をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 7 月 9 日 17:08 UTC
- 編集日時: 2015 年 7 月 9 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IVSFullAccess

説明：インタラクティブビデオサービス (IVS) へのフルアクセスを提供します。また、ivs コンソールへのフルアクセスに必要な、依存サービスのアクセス許可も含まれています。

IVSFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに IVSFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 13 日 21:20 UTC
- 編集日時: 2023 年 12 月 13 日 21:20 UTC

- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IVSReadOnlyAccess

説明: IVS 低レイテンシーおよびリアルタイムストリーミング APIs

IVSReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに `IVSReadOnlyAccess` をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 12 月 5 日 18:00 UTC
- 編集日時: 2024 年 2 月 16 日 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

IVSRecordToS3

説明： IVS ライブストリームを記録する S3 PutObject を実行するサービスリンクロール

IVSRecordToS3 は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 12 月 5 日 00:10 UTC
- 編集日時: 2020 年 12 月 5 日 00:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

KafkaConnectServiceRolePolicy

説明：このポリシーは、ユーザーに代わって AWS リソースを管理するアクセス許可を Kafka Connect に付与します。

KafkaConnectServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 9 月 7 日 13:12 UTC
- 編集日時: 2021 年 9 月 7 日 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

KafkaServiceRolePolicy

説明： Kafka の IAM サービスにリンクされたロールポリシー。

KafkaServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 11 月 15 日 23:31 UTC
- 編集日時: 2023 年 4 月 28 日 00:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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_*"
    }
  }
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

KeyspacesReplicationServiceRolePolicy

説明：クロスリージョンデータレプリケーションに Keyspaces で必要なアクセス許可

KeyspacesReplicationServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 5 月 2 日 16:15 UTC
- 編集日時: 2023 年 5 月 2 日 16:15 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

LakeFormationDataAccessServiceRolePolicy

説明: Lake Formation リソースへの一時データアクセスを許可するポリシー

LakeFormationDataAccessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 20 日 20:46 UTC
- 編集日時: 2024 年 2 月 6 日 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

LexBotPolicy

説明: AWS Lex Bot ユースケースのポリシー

LexBotPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2017 年 2 月 17 日 22:18 UTC
- 編集日時: 2019 年 11 月 13 日 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "polly:SynthesizeSpeech"
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "comprehend:DetectSentiment"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

LexChannelPolicy

説明: AWS Lex Channel ユースケースのポリシー

LexChannelPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2017 年 2 月 17 日 23:23 UTC
- 編集日時: 2017 年 2 月 17 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

LightsailExportAccess

説明: リソースをエクスポートするアクセス許可を付与する AWS Lightsail サービスにリンクされたロールポリシー

LightsailExportAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 9 月 28 日 16:35 UTC
- 編集日時: 2022 年 1 月 15 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

MediaConnectGatewayInstanceRolePolicy

説明：このポリシーは、MediaConnect ゲートウェイインスタンスを MediaConnect ゲートウェイに登録するアクセス許可を付与します。

MediaConnectGatewayInstanceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに MediaConnectGatewayInstanceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 22 日 20:43 UTC
- 編集日時: 2023 年 3 月 22 日 20:43 UTC
- ARN: arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediacconnect:DiscoverGatewayPollEndpoint",
        "mediacconnect:PollGateway",
        "mediacconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

MediaPackageServiceRolePolicy

説明 : が MediaPackage にログを発行することを許可する CloudWatch

MediaPackageServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 9 月 18 日 17:45 UTC
- 編集日時: 2020 年 9 月 18 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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/*"  
  }  
]  
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

MemoryDBServiceRolePolicy

説明： このポリシーにより、MemoryDB は AWS、リソースを管理するために必要なリソースをユーザーに代わって管理できます。

MemoryDBServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 8 月 17 日 22:34 UTC
- 編集日時: 2021 年 8 月 18 日 23:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

ポリシーのバージョニング

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

MigrationHubDMSAccessServiceRolePolicy

説明: Database Migration Service が Migration Hub を呼び出すためにお客様のアカウントでロールを引き受けるためのポリシー

MigrationHubDMSAccessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:50 UTC
- 編集日時: 2019 年 10 月 7 日 17:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

MigrationHubServiceRolePolicy

説明 : Migration Hub がユーザーに代わって Application Discovery Service を呼び出すことを許可します

MigrationHubServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 17:22 UTC
- 編集日時: 2020 年 8 月 6 日 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
    "*"
  ]
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

MigrationHubSMSAccessServiceRolePolicy

説明：お客様のアカウントで Migration Hub を呼び出すためのロールを引き受けるための Server Migration Service のポリシー

MigrationHubSMSAccessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 6 月 12 日 18:30 UTC
- 編集日時: 2019 年 10 月 7 日 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

MonitronServiceRolePolicy

説明：必要なカスタマーリソースへのアクセスを許可する AWS Monitron サービスにリンクされたロールのポリシー。

MonitronServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 5 月 2 日 19:22 UTC
- 編集日時: 2022 年 5 月 2 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

NeptuneConsoleFullAccess

説明： を使用して Amazon Neptune を管理するためのフルアクセスを提供します AWS Management Console。このポリシーでは、アカウント内のすべての SNS トピックを公開するためのフルアクセス、Amazon EC2 インスタンスおよび VPC 設定を作成および編集する許可、Amazon KMS でキーを表示および一覧表示する許可、Amazon RDS へのフルアクセスも付与されることにご注意ください。詳細については、<https://aws.amazon.com/neptune/faqs/> を参照してください。

NeptuneConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 6 月 19 日 21:35 UTC
- 編集日時: 2023 年 11 月 30 日 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:RemoveTagsForResource",
"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"
    }
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

NeptuneFullAccess

説明： Amazon Neptune へのフルアクセスを提供します。このポリシーでは、アカウント内のすべての SNS トピックに公開するためのフルアクセスおよび Amazon RDS へのフルアクセスも付与されることにご注意ください。詳細については、<https://aws.amazon.com/neptune/faqs/> を参照してください。

NeptuneFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 5 月 30 日 19:17 UTC

- 編集日時 : 2024 年 1 月 22 日 16:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneFullAccess

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:RemoveTagsForResource",
    "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" : [
    "*"
  ]
}
```

```
    ]
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

NeptuneGraphReadOnlyAccess

説明：すべての Amazon Neptune Analytics リソースへの読み取り専用アクセスと、依存サービスの読み取り専用アクセス許可を提供します。

NeptuneGraphReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneGraphReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 30 日 07:32 UTC
- 編集日時: 2023 年 11 月 30 日 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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:*"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

NeptuneReadOnlyAccess

説明： Amazon Neptune への読み取り専用アクセスを提供します。このポリシーでは、Amazon RDS リソースへのアクセスも付与されることにご注意ください。詳細については、<https://aws.amazon.com/neptune/faqs/> を参照してください。

NeptuneReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに NeptuneReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2018 年 5 月 30 日 19:16 UTC
- 編集日時: 2024 年 1 月 22 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : [
      "*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

NetworkAdministrator

説明: AWS ネットワークリソースの設定と設定に必要な AWS サービスとアクションへのフルアクセス許可を付与します。

NetworkAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに NetworkAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:31 UTC
- 編集日時: 2021 年 9 月 16 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

ポリシーのバージョン

ポリシーのバージョン: v11 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      ]
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

OAMFullAccess

説明： Observability Access Manager CloudWatch へのフルアクセスを提供します

OAMFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに OAMFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:38 UTC
- 編集日時: 2022 年 11 月 27 日 13:38 UTC
- ARN: arn:aws:iam::aws:policy/OAMFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
    }
  ],
}
```



```
    "Resource" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

OAMReadOnlyAccess

説明： Observability Access Manager CloudWatch への読み取り専用アクセスを提供します

OAMReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに OAMReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 11 月 27 日 13:29 UTC
- 編集日時: 2022 年 11 月 27 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

OpensearchIngestionSelfManagedVpcePolicy

説明： Amazon OpenSearch Ingestion がネットワークリソースを記述し、サービスマトリクスを cloudwatch に書き込むことを許可します

OpensearchIngestionSelfManagedVpcePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2024 年 6 月 10 日 19:59 UTC
- 編集日時: 2024 年 6 月 10 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

PartnerCentralAccountManagementUserRoleAssociation

説明： パートナーセントラルユーザーを IAM ロールに関連付けたり関連付けを解除したりするためのアクセスを提供します

PartnerCentralAccountManagementUserRoleAssociation は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

PartnerCentralAccountManagementUserRoleAssociation をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 11 月 10 日 02:03 UTC
- 編集日時: 2023 年 11 月 10 日 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

PowerUserAccess

説明：AWS サービスとリソースへのフルアクセスを提供しますが、ユーザーとグループの管理は許可しません。

PowerUserAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに PowerUserAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 7 月 6 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

QBusinessServiceRolePolicy

説明: Amazon Q が使用または管理する AWS のサービス およびリソースにアクセス許可を付与します

QBusinessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー

- 作成日時: 2024 年 4 月 29 日 16:05 UTC
- 編集日時: 2024 年 4 月 29 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
```



```
        "aws:ResourceAccount" : "${aws:PrincipalAccount}"
    }
}
},
{
    "Sid" : "QBusinessDescribeLogGroupsPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogGroups"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid" : "QBusinessLogStreamPermission",
    "Effect" : "Allow",
    "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
    ],
    "Condition" : {
        "StringEquals" : {
            "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
    }
}
]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

説明: S3 Storage Management Analytics によって生成された顧客データにアクセスするために QuickSight チームが使用するポリシー。

QuickSightAccessForS3StorageManagementAnalyticsReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに

QuickSightAccessForS3StorageManagementAnalyticsReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2017 年 6 月 12 日 18:18 UTC
- 編集日時: 2019 年 10 月 8 日 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

RDSCloudHsmAuthorizationRole

説明： Amazon RDS サービスロールのデフォルトポリシー。

RDSCloudHsmAuthorizationRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに RDSCloudHsmAuthorizationRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2019 年 9 月 26 日 22:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ReadOnlyAccess

説明：AWS サービスとリソースへの読み取り専用アクセスを提供します。

ReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2024 年 5 月 16 日 21:10 UTC
- ARN: arn:aws:iam::aws:policy/ReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v113 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",

```

```
"access-analyzer:ListAccessPreviews",
"access-analyzer:ListAnalyzedResources",
"access-analyzer:ListAnalyzers",
"access-analyzer:ListArchiveRules",
"access-analyzer:ListFindings",
"access-analyzer:ListPolicyGenerations",
"access-analyzer:ListTagsForResource",
"access-analyzer:ValidatePolicy",
"account:GetAccountInformation",
"account:GetAlternateContact",
"account:GetChallengeQuestions",
"account:GetContactInformation",
"account:GetRegionOptStatus",
"account:ListRegions",
"acm-pca:Describe*",
"acm-pca:Get*",
"acm-pca:List*",
"acm:Describe*",
"acm:Get*",
"acm:List*",
"airflow:ListEnvironments",
"airflow:ListTagsForResource",
"amplify:GetApp",
"amplify:GetBranch",
"amplify:GetDomainAssociation",
"amplify:GetJob",
"amplify:ListApps",
"amplify:ListBranches",
"amplify:ListDomainAssociations",
"amplify:ListJobs",
"aoss:BatchGetCollection",
"aoss:BatchGetLifecyclePolicy",
"aoss:BatchGetVpcEndpoint",
"aoss:GetAccessPolicy",
"aoss:GetAccountSettings",
"aoss:GetPoliciesStats",
"aoss:GetSecurityConfig",
"aoss:GetSecurityPolicy",
"aoss:ListAccessPolicies",
"aoss:ListCollections",
"aoss:ListLifecyclePolicies",
"aoss:ListSecurityConfigs",
"aoss:ListSecurityPolicies",
"aoss:ListTagsForResource",
```

```
"aoss:ListVpcEndpoints",
"apigateway:GET",
"appconfig:GetApplication",
"appconfig:GetConfiguration",
"appconfig:GetConfigurationProfile",
"appconfig:GetDeployment",
"appconfig:GetDeploymentStrategy",
"appconfig:GetEnvironment",
"appconfig:GetHostedConfigurationVersion",
"appconfig:ListApplications",
"appconfig:ListConfigurationProfiles",
"appconfig:ListDeployments",
"appconfig:ListDeploymentStrategies",
"appconfig:ListEnvironments",
"appconfig:ListHostedConfigurationVersions",
"appconfig:ListTagsForResource",
"appfabric:GetAppAuthorization",
"appfabric:GetAppBundle",
"appfabric:GetIngestion",
"appfabric:GetIngestionDestination",
"appfabric:ListAppAuthorizations",
"appfabric:ListAppBundles",
"appfabric:ListIngestionDestinations",
"appfabric:ListIngestions",
"appfabric:ListTagsForResource",
"appflow:DescribeConnector",
"appflow:DescribeConnectorEntity",
"appflow:DescribeConnectorFields",
"appflow:DescribeConnectorProfiles",
"appflow:DescribeConnectors",
"appflow:DescribeFlow",
"appflow:DescribeFlowExecution",
"appflow:DescribeFlowExecutionRecords",
"appflow:DescribeFlows",
"appflow:ListConnectorEntities",
"appflow:ListConnectorFields",
"appflow:ListConnectors",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:Describe*",
"application-autoscaling:ListTagsForResource",
"applicationinsights:Describe*",
"applicationinsights:List*",
"appmesh:Describe*",
```

```
"appmesh:List*",
"apprunner:DescribeAutoScalingConfiguration",
"apprunner:DescribeCustomDomains",
"apprunner:DescribeObservabilityConfiguration",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:DescribeVpcIngressConnection",
"apprunner:DescribeWebAclForService",
"apprunner:ListAssociatedServicesForWebAcl",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListServicesForAutoScalingConfiguration",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appstream:Describe*",
"appstream:List*",
"appsync:Get*",
"appsync:List*",
"aps:DescribeAlertManagerDefinition",
"aps:DescribeLoggingConfiguration",
"aps:DescribeRuleGroupsNamespace",
"aps:DescribeScraper",
"aps:DescribeWorkspace",
"aps:GetAlertManagerSilence",
"aps:GetAlertManagerStatus",
"aps:GetDefaultScraperConfiguration",
"aps:GetLabels",
"aps:GetMetricMetadata",
"aps:GetSeries",
"aps:ListAlertManagerAlertGroups",
"aps:ListAlertManagerAlerts",
"aps:ListAlertManagerReceivers",
"aps:ListAlertManagerSilences",
"aps:ListAlerts",
"aps:ListRuleGroupsNamespaces",
"aps:ListRules",
"aps:ListScrapers",
"aps:ListTagsForResource",
"aps:ListWorkspaces",
"aps:QueryMetrics",
```



```
"arc-zonal-shift:GetManagedResource",
"arc-zonal-shift:ListAutoshifts",
"arc-zonal-shift:ListManagedResources",
"arc-zonal-shift:ListZonalShifts",
"artifact:GetReport",
"artifact:GetReportMetadata",
"artifact:GetTermForReport",
"artifact:ListReports",
"athena:Batch*",
"athena:Get*",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:GetAssessment",
"auditmanager:GetAssessmentFramework",
"auditmanager:GetAssessmentReportUrl",
"auditmanager:GetChangeLogs",
"auditmanager:GetControl",
"auditmanager:GetDelegations",
"auditmanager:GetEvidence",
"auditmanager:GetEvidenceByEvidenceFolder",
"auditmanager:GetEvidenceFolder",
"auditmanager:GetEvidenceFoldersByAssessment",
"auditmanager:GetEvidenceFoldersByAssessmentControl",
"auditmanager:GetOrganizationAdminAccount",
"auditmanager:GetServicesInScope",
"auditmanager:GetSettings",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControls",
"auditmanager:ListKeywordsForDataSource",
"auditmanager:ListNotifications",
"auditmanager:ListTagsForResource",
"auditmanager:ValidateAssessmentReportIntegrity",
"autoscaling-plans:Describe*",
"autoscaling-plans:GetScalingPlanResourceForecastData",
"autoscaling:Describe*",
"autoscaling:GetPredictiveScalingForecast",
"aws-portal:View*",
"backup-gateway:GetBandwidthRateLimitSchedule",
"backup-gateway:GetGateway",
"backup-gateway:GetHypervisor",
"backup-gateway:GetHypervisorPropertyMappings",
"backup-gateway:GetVirtualMachine",
```

```
"backup-gateway:ListGateways",
"backup-gateway:ListHypervisors",
"backup-gateway:ListTagsForResource",
"backup-gateway:ListVirtualMachines",
"backup:Describe*",
"backup:Get*",
"backup:List*",
"batch:Describe*",
"batch:List*",
"bedrock:GetAgent",
"bedrock:GetAgentActionGroup",
"bedrock:GetAgentAlias",
"bedrock:GetAgentKnowledgeBase",
"bedrock:GetAgentVersion",
"bedrock:GetCustomModel",
"bedrock:GetDataSource",
"bedrock:GetFoundationModel",
"bedrock:GetFoundationModelAvailability",
"bedrock:GetIngestionJob",
"bedrock:GetKnowledgeBase",
"bedrock:GetModelCustomizationJob",
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:GetProvisionedModelThroughput",
"bedrock:GetUseCaseForModelAccess",
"bedrock:ListAgentActionGroups",
"bedrock:ListAgentAliases",
"bedrock:ListAgentKnowledgeBases",
"bedrock:ListAgents",
"bedrock:ListAgentVersions",
"bedrock:ListCustomModels",
"bedrock:ListDataSources",
"bedrock:ListFoundationModelAgreementOffers",
"bedrock:ListFoundationModels",
"bedrock:ListIngestionJobs",
"bedrock:ListKnowledgeBases",
"bedrock:ListModelCustomizationJobs",
"bedrock:ListProvisionedModelThroughputs",
"billing:GetBillingData",
"billing:GetBillingDetails",
"billing:GetBillingNotifications",
"billing:GetBillingPreferences",
"billing:GetContractInformation",
"billing:GetCredits",
"billing:GetIAMAccessPreference",
```

```
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"billingconductor:GetBillingGroupCostReport",
"billingconductor:ListAccountAssociations",
"billingconductor:ListBillingGroupCostReports",
"billingconductor:ListBillingGroups",
"billingconductor:ListCustomLineItems",
"billingconductor:ListCustomLineItemVersions",
"billingconductor:ListPricingPlans",
"billingconductor:ListPricingPlansAssociatedWithPricingRule",
"billingconductor:ListPricingRules",
"billingconductor:ListPricingRulesAssociatedToPricingPlan",
"billingconductor:ListResourcesAssociatedToCustomLineItem",
"billingconductor:ListTagsForResource",
"braket:GetDevice",
"braket:GetJob",
"braket:GetQuantumTask",
"braket:SearchDevices",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"budgets:Describe*",
"budgets:View*",
"cassandra:Select",
"ce:DescribeCostCategoryDefinition",
"ce:DescribeNotificationSubscription",
"ce:DescribeReport",
"ce:GetAnomalies",
"ce:GetAnomalyMonitors",
"ce:GetAnomalySubscriptions",
"ce:GetApproximateUsageRecords",
"ce:GetCostAndUsage",
"ce:GetCostAndUsageWithResources",
"ce:GetCostCategories",
"ce:GetCostForecast",
"ce:GetDimensionValues",
"ce:GetPreferences",
"ce:GetReservationCoverage",
"ce:GetReservationPurchaseRecommendation",
"ce:GetReservationUtilization",
"ce:GetRightsizingRecommendation",
"ce:GetSavingsPlanPurchaseRecommendationDetails",
"ce:GetSavingsPlansCoverage",
"ce:GetSavingsPlansPurchaseRecommendation",
"ce:GetSavingsPlansUtilization",
```

```
"ce:GetSavingsPlansUtilizationDetails",
"ce:GetTags",
"ce:GetUsageForecast",
"ce:ListCostAllocationTags",
"ce:ListCostAllocationTagBackfillHistory",
"ce:ListCostCategoryDefinitions",
"ce:ListSavingsPlansPurchaseRecommendationGeneration",
"ce:ListTagsForResource",
"chatbot:Describe*",
"chatbot:Get*",
"chatbot:ListMicrosoftTeamsChannelConfigurations",
"chatbot:ListMicrosoftTeamsConfiguredTeams",
"chatbot:ListMicrosoftTeamsUserIdentities",
"chime:Get*",
"chime:List*",
"chime:Retrieve*",
"chime:Search*",
"chime:Validate*",
"cleanrooms:BatchGetCollaborationAnalysisTemplate",
"cleanrooms:BatchGetSchema",
"cleanrooms:GetAnalysisTemplate",
"cleanrooms:GetCollaboration",
"cleanrooms:GetCollaborationAnalysisTemplate",
"cleanrooms:GetConfiguredAudienceModelAssociation",
"cleanrooms:GetConfiguredTable",
"cleanrooms:GetConfiguredTableAnalysisRule",
"cleanrooms:GetConfiguredTableAssociation",
"cleanrooms:GetMembership",
"cleanrooms:GetProtectedQuery",
"cleanrooms:GetSchema",
"cleanrooms:GetSchemaAnalysisRule",
"cleanrooms:ListAnalysisTemplates",
"cleanrooms:ListCollaborationAnalysisTemplates",
"cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
"cleanrooms:ListCollaborations",
"cleanrooms:ListConfiguredTableAssociations",
"cleanrooms:ListConfiguredTables",
"cleanrooms:ListMembers",
"cleanrooms:ListMemberships",
"cleanrooms:ListProtectedQueries",
"cleanrooms:ListSchemas",
"cleanrooms:ListTagsForResource",
"cleanrooms-ml:GetTrainingDataset",
"cleanrooms-ml:GetAudienceGenerationJob",
```

```
"cleanrooms-ml:GetAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModel",
"cleanrooms-ml:GetConfiguredAudienceModelPolicy",
"cleanrooms-ml:ListAudienceExportJobs",
"cleanrooms-ml:ListAudienceGenerationJobs",
"cleanrooms-ml:ListAudienceModels",
"cleanrooms-ml:ListConfiguredAudienceModels",
"cleanrooms-ml:ListTrainingDatasets",
"cleanrooms-ml:ListTagsForResource",
"cloud9:Describe*",
"cloud9:List*",
"clouddirectory:BatchRead",
"clouddirectory:Get*",
"clouddirectory:List*",
"clouddirectory:LookupPolicy",
"cloudformation:Describe*",
"cloudformation:Detect*",
"cloudformation:Estimate*",
"cloudformation:Get*",
"cloudformation:List*",
"cloudformation:ValidateTemplate",
"cloudfront-keyvaluestore:Describe*",
"cloudfront-keyvaluestore:Get*",
"cloudfront-keyvaluestore:List*",
"cloudfront:Describe*",
"cloudfront:Get*",
"cloudfront:List*",
"cloudhsm:Describe*",
"cloudhsm:List*",
"cloudsearch:Describe*",
"cloudsearch:List*",
"cloudtrail:Describe*",
"cloudtrail:Get*",
"cloudtrail:List*",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"codeartifact:DescribeDomain",
"codeartifact:DescribePackage",
"codeartifact:DescribePackageVersion",
"codeartifact:DescribeRepository",
"codeartifact:GetAuthorizationToken",
```

```
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetPackageVersionAsset",
"codeartifact:GetPackageVersionReadme",
"codeartifact:GetRepositoryEndpoint",
"codeartifact:GetRepositoryPermissionsPolicy",
"codeartifact:ListDomains",
"codeartifact:ListPackages",
"codeartifact:ListPackageVersionAssets",
"codeartifact:ListPackageVersionDependencies",
"codeartifact:ListPackageVersions",
"codeartifact:ListRepositories",
"codeartifact:ListRepositoriesInDomain",
"codeartifact:ListTagsForResource",
"codeartifact:ReadFromRepository",
"codebuild:BatchGet*",
"codebuild:DescribeCodeCoverages",
"codebuild:DescribeTestCases",
"codebuild:List*",
"codecatalyst:GetBillingAuthorization",
"codecatalyst:GetConnection",
"codecatalyst:GetPendingConnection",
"codecatalyst:ListConnections",
"codecatalyst:ListIamRolesForConnection",
"codecatalyst:ListTagsForResource",
"codecommit:BatchGet*",
"codecommit:Describe*",
"codecommit:Get*",
"codecommit:GitPull",
"codecommit:List*",
"codedeploy:BatchGet*",
"codedeploy:Get*",
"codedeploy:List*",
"codeguru-profiler:Describe*",
"codeguru-profiler:Get*",
"codeguru-profiler:List*",
"codeguru-reviewer:Describe*",
"codeguru-reviewer:Get*",
"codeguru-reviewer:List*",
"codepipeline:Get*",
"codepipeline:List*",
"codestar-connections:GetConnection",
"codestar-connections:GetHost",
"codestar-connections:GetRepositoryLink",
"codestar-connections:GetRepositorySyncStatus",
```

```
"codestar-connections:GetResourceSyncStatus",
"codestar-connections:GetSyncConfiguration",
"codestar-connections:ListConnections",
"codestar-connections:ListHosts",
"codestar-connections:ListRepositoryLinks",
"codestar-connections:ListRepositorySyncDefinitions",
"codestar-connections:ListSyncConfigurations",
"codestar-connections:ListTagsForResource",
"codestar-notifications:describeNotificationRule",
"codestar-notifications:listEventTypes",
"codestar-notifications:listNotificationRules",
"codestar-notifications:listTagsForResource",
"codestar-notifications:ListTargets",
"codestar:Describe*",
"codestar:Get*",
"codestar:List*",
"codestar:Verify*",
"cognito-identity:Describe*",
"cognito-identity:GetCredentialsForIdentity",
"cognito-identity:GetIdentityPoolAnalytics",
"cognito-identity:GetIdentityPoolDailyAnalytics",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:GetIdentityProviderDailyAnalytics",
"cognito-identity:GetOpenIdToken",
"cognito-identity:GetOpenIdTokenForDeveloperIdentity",
"cognito-identity:List*",
"cognito-identity:Lookup*",
"cognito-idp:AdminGet*",
"cognito-idp:AdminList*",
"cognito-idp:Describe*",
"cognito-idp:Get*",
"cognito-idp:List*",
"cognito-sync:Describe*",
"cognito-sync:Get*",
"cognito-sync:List*",
"cognito-sync:QueryRecords",
"comprehend:BatchDetect*",
"comprehend:Classify*",
"comprehend:Contains*",
"comprehend:Describe*",
"comprehend:Detect*",
"comprehend:List*",
"compute-optimizer:DescribeRecommendationExportJobs",
"compute-optimizer:GetAutoScalingGroupRecommendations",
```

```
"compute-optimizer:GetEBSVolumeRecommendations",
"compute-optimizer:GetEC2InstanceRecommendations",
"compute-optimizer:GetEC2RecommendationProjectedMetrics",
"compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
"compute-optimizer:GetECSServiceRecommendations",
"compute-optimizer:GetEffectiveRecommendationPreferences",
"compute-optimizer:GetEnrollmentStatus",
"compute-optimizer:GetEnrollmentStatusesForOrganization",
"compute-optimizer:GetLambdaFunctionRecommendations",
"compute-optimizer:GetLicenseRecommendations",
"compute-optimizer:GetRecommendationPreferences",
"compute-optimizer:GetRecommendationSummaries",
"config:BatchGetAggregateResourceConfig",
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config:SelectAggregateResourceConfig",
"config:SelectResourceConfig",
"connect:Describe*",
"connect:GetContactAttributes",
"connect:GetCurrentMetricData",
"connect:GetCurrentUserData",
"connect:GetFederationToken",
"connect:GetMetricData",
"connect:GetMetricDataV2",
"connect:GetTaskTemplate",
"connect:GetTrafficDistribution",
"connect:List*",
"consoleapp:GetDeviceIdentity",
"consoleapp:ListDeviceIdentities",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendations",
"cost-optimization-hub:ListRecommendationSummaries",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"customer-verification:GetCustomerVerificationDetails",
"customer-verification:GetCustomerVerificationEligibility",
```



```
"databrew:DescribeDataset",
"databrew:DescribeJob",
"databrew:DescribeJobRun",
"databrew:DescribeProject",
"databrew:DescribeRecipe",
"databrew:DescribeRuleset",
"databrew:DescribeSchedule",
"databrew:ListDatasets",
"databrew:ListJobRuns",
"databrew:ListJobs",
"databrew:ListProjects",
"databrew:ListRecipes",
"databrew:ListRecipeVersions",
"databrew:ListRulesets",
"databrew:ListSchedules",
"databrew:ListTagsForResource",
"dataexchange:Get*",
"dataexchange:List*",
"datapipeline:Describe*",
"datapipeline:EvaluateExpression",
"datapipeline:Get*",
"datapipeline:List*",
"datapipeline:QueryObjects",
"datapipeline:Validate*",
"datasync:Describe*",
"datasync:List*",
"dax:BatchGetItem",
"dax:Describe*",
"dax:GetItem",
"dax:ListTags",
"dax:Query",
"dax:Scan",
"deadline:BatchGetJobEntity",
"deadline:GetApplicationVersion",
"deadline:GetBudget",
"deadline:GetFarm",
"deadline:GetFleet",
"deadline:GetJob",
"deadline:GetLicenseEndpoint",
"deadline:GetMonitor",
"deadline:GetQueue",
"deadline:GetQueueEnvironment",
"deadline:GetQueueFleetAssociation",
"deadline:GetSession",
```

```
"deadline:GetSessionAction",
"deadline:GetSessionsStatisticsAggregation",
"deadline:GetStep",
"deadline:GetStorageProfile",
"deadline:GetStorageProfileForQueue",
"deadline:GetTask",
"deadline:GetWorker",
"deadline:ListAvailableMeteredProducts",
"deadline:ListBudgets",
"deadline:ListFarmMembers",
"deadline:ListFarms",
"deadline:ListFleetMembers",
"deadline:ListFleets",
"deadline:ListJobMembers",
"deadline:ListJobs",
"deadline:ListLicenseEndpoints",
"deadline:ListMeteredProducts",
"deadline:ListMonitors",
"deadline:ListQueueEnvironments",
"deadline:ListQueueFleetAssociations",
"deadline:ListQueueMembers",
"deadline:ListQueues",
"deadline:ListSessionActions",
"deadline:ListSessions",
"deadline:ListSessionsForWorker",
"deadline:ListStepConsumers",
"deadline:ListStepDependencies",
"deadline:ListSteps",
"deadline:ListStorageProfiles",
"deadline:ListStorageProfilesForQueue",
"deadline:ListTagsForResource",
"deadline:ListTasks",
"deadline:ListWorkers",
"deadline:SearchJobs",
"deadline:SearchSteps",
"deadline:SearchTasks",
"deadline:SearchWorkers",
"deepcomposer:GetComposition",
"deepcomposer:GetModel",
"deepcomposer:GetSampleModel",
"deepcomposer:ListCompositions",
"deepcomposer:ListModels",
"deepcomposer:ListSampleModels",
"deepcomposer:ListTrainingTopics",
```

```
"detective:BatchGetGraphMemberDatasources",
"detective:BatchGetMembershipDatasources",
"detective:Get*",
"detective:List*",
"detective:SearchGraph",
"devicefarm:Get*",
"devicefarm:List*",
"devops-guru:DescribeAccountHealth",
"devops-guru:DescribeAccountOverview",
"devops-guru:DescribeAnomaly",
"devops-guru:DescribeEventSourcesConfig",
"devops-guru:DescribeFeedback",
"devops-guru:DescribeInsight",
"devops-guru:DescribeOrganizationHealth",
"devops-guru:DescribeOrganizationOverview",
"devops-guru:DescribeOrganizationResourceCollectionHealth",
"devops-guru:DescribeResourceCollectionHealth",
"devops-guru:DescribeServiceIntegration",
"devops-guru:GetCostEstimation",
"devops-guru:GetResourceCollection",
"devops-guru:ListAnomaliesForInsight",
"devops-guru:ListAnomalousLogGroups",
"devops-guru:ListEvents",
"devops-guru:ListInsights",
"devops-guru:ListMonitoredResources",
"devops-guru:ListNotificationChannels",
"devops-guru:ListOrganizationInsights",
"devops-guru:ListRecommendations",
"devops-guru:SearchInsights",
"devops-guru:StartCostEstimation",
"directconnect:Describe*",
"discovery:Describe*",
"discovery:Get*",
"discovery:List*",
"dlm:Get*",
"dms:Describe*",
"dms:List*",
"dms:Test*",
"drs:DescribeJobLogItems",
"drs:DescribeJobs",
"drs:DescribeLaunchConfigurationTemplates",
"drs:DescribeRecoveryInstances",
"drs:DescribeRecoverySnapshots",
"drs:DescribeReplicationConfigurationTemplates",
```

```
"drs:DescribeSourceNetworks",
"drs:DescribeSourceServers",
"drs:GetFailbackReplicationConfiguration",
"drs:GetLaunchConfiguration",
"drs:GetReplicationConfiguration",
"drs:ListExtensibleSourceServers",
"drs:ListLaunchActions",
"drs:ListStagingAccounts",
"drs:ListTagsForResource",
"ds:Check*",
"ds:Describe*",
"ds:Get*",
"ds:List*",
"ds:Verify*",
"dynamodb:BatchGet*",
"dynamodb:Describe*",
"dynamodb:Get*",
"dynamodb:List*",
"dynamodb: PartiQLSelect",
"dynamodb:Query",
"dynamodb:Scan",
"ec2:Describe*",
"ec2:Get*",
"ec2:ListImagesInRecycleBin",
"ec2:ListSnapshotsInRecycleBin",
"ec2:SearchLocalGatewayRoutes",
"ec2:SearchTransitGatewayRoutes",
"ec2messages:Get*",
"ecr-public:BatchCheckLayerAvailability",
"ecr-public:DescribeImages",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetAuthorizationToken",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchCheck*",
"ecr:BatchGet*",
"ecr:Describe*",
"ecr:Get*",
"ecr:List*",
"ecs:Describe*",
```

```
"ecs:List*",
"eks:Describe*",
"eks:List*",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAccelerators",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticache:List*",
"elasticbeanstalk:Check*",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:List*",
"elasticbeanstalk:Request*",
"elasticbeanstalk:Retrieve*",
"elasticbeanstalk:Validate*",
"elasticfilesystem:Describe*",
"elasticfilesystem:ListTagsForResource",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:List*",
"elasticmapreduce:View*",
"elastictranscoder:List*",
"elastictranscoder:Read*",
"elemental-appliances-software:Get*",
"elemental-appliances-software:List*",
"emr-containers:DescribeJobRun",
"emr-containers:DescribeManagedEndpoint",
"emr-containers:DescribeVirtualCluster",
"emr-containers:ListJobRuns",
"emr-containers:ListManagedEndpoints",
"emr-containers:ListTagsForResource",
"emr-containers:ListVirtualClusters",
"emr-serverless:GetApplication",
"emr-serverless:GetDashboardForJobRun",
"emr-serverless:GetJobRun",
"emr-serverless:ListApplications",
"emr-serverless:ListJobRuns",
"emr-serverless:ListTagsForResource",
"es:Describe*",
"es:ESHttpGet",
"es:ESHttpHead",
"es:Get*",
"es:List*",
```

```
"events:Describe*",
"events:List*",
"events:Test*",
"evidently:GetExperiment",
"evidently:GetExperimentResults",
"evidently:GetFeature",
"evidently:GetLaunch",
"evidently:GetProject",
"evidently:GetSegment",
"evidently:ListExperiments",
"evidently:ListFeatures",
"evidently:ListLaunches",
"evidently:ListProjects",
"evidently:ListSegmentReferences",
"evidently:ListSegments",
"evidently:ListTagsForResource",
"evidently:TestSegmentPattern",
"firehose:Describe*",
"firehose:List*",
"fis:GetAction",
"fis:GetExperiment",
"fis:GetExperimentTargetAccountConfiguration",
"fis:GetExperimentTemplate",
"fis:GetTargetAccountConfiguration",
"fis:GetTargetResourceType",
"fis:ListActions",
"fis:ListExperimentResolvedTargets",
"fis:ListExperiments",
"fis:ListExperimentTargetAccountConfigurations",
"fis:ListExperimentTemplates",
"fis:ListTagsForResource",
"fis:ListTargetAccountConfigurations",
"fis:ListTargetResourceTypes",
"fms:GetAdminAccount",
"fms:GetAppsList",
"fms:GetComplianceDetail",
"fms:GetNotificationChannel",
"fms:GetPolicy",
"fms:GetProtectionStatus",
"fms:GetProtocolsList",
"fms:GetViolationDetails",
"fms:ListAppsLists",
"fms:ListComplianceStatus",
"fms:ListMemberAccounts",
```

```
"fms:ListPolicies",
"fms:ListProtocolsLists",
"fms:ListTagsForResource",
"forecast:DescribeAutoPredictor",
"forecast:DescribeDataset",
"forecast:DescribeDatasetGroup",
"forecast:DescribeDatasetImportJob",
"forecast:DescribeExplainability",
"forecast:DescribeExplainabilityExport",
"forecast:DescribeForecast",
"forecast:DescribeForecastExportJob",
"forecast:DescribeMonitor",
"forecast:DescribePredictor",
"forecast:DescribePredictorBacktestExportJob",
"forecast:DescribeWhatIfAnalysis",
"forecast:DescribeWhatIfForecast",
"forecast:DescribeWhatIfForecastExport",
"forecast:GetAccuracyMetrics",
"forecast:ListDatasetGroups",
"forecast:ListDatasetImportJobs",
"forecast:ListDatasets",
"forecast:ListExplainabilities",
"forecast:ListExplainabilityExports",
"forecast:ListForecastExportJobs",
"forecast:ListForecasts",
"forecast:ListMonitorEvaluations",
"forecast:ListMonitors",
"forecast:ListPredictorBacktestExportJobs",
"forecast:ListPredictors",
"forecast:ListWhatIfAnalyses",
"forecast:ListWhatIfForecastExports",
"forecast:ListWhatIfForecasts",
"forecast:QueryForecast",
"forecast:QueryWhatIfForecast",
"frauddetector:BatchGetVariable",
"frauddetector:DescribeDetector",
"frauddetector:DescribeModelVersions",
"frauddetector:GetBatchImportJobs",
"frauddetector:GetBatchPredictionJobs",
"frauddetector:GetDeleteEventsByEventTypeStatus",
"frauddetector:GetDetectors",
"frauddetector:GetDetectorVersion",
"frauddetector:GetEntityTypes",
"frauddetector:GetEvent",
```

```
"frauddetector:GetEventPredictionMetadata",
"frauddetector:GetEventTypes",
"frauddetector:GetExternalModels",
"frauddetector:GetKMSEncryptionKey",
"frauddetector:GetLabels",
"frauddetector:GetListElements",
"frauddetector:GetListsMetadata",
"frauddetector:GetModels",
"frauddetector:GetModelVersion",
"frauddetector:GetOutcomes",
"frauddetector:GetRules",
"frauddetector:GetVariables",
"frauddetector:ListEventPredictions",
"frauddetector:ListTagsForResource",
"freertos:Describe*",
"freertos:List*",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"fsx:Describe*",
"fsx:List*",
"gamelift:Describe*",
"gamelift:Get*",
"gamelift:List*",
"gamelift:ResolveAlias",
"gamelift:Search*",
"glacier:Describe*",
"glacier:Get*",
"glacier:List*",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:BatchGetCrawlers",
"glue:BatchGetDevEndpoints",
"glue:BatchGetJobs",
"glue:BatchGetPartition",
"glue:BatchGetTriggers",
"glue:BatchGetWorkflows",
"glue:CheckSchemaVersionValidity",
"glue:GetCatalogImportStatus",
"glue:GetClassifier",
"glue:GetClassifiers",
"glue:GetCrawler",
"glue:GetCrawlerMetrics",
"glue:GetCrawlers",
"glue:GetDatabase",
```



```
"glue:GetDatabases",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDataflowGraph",
"glue:GetDevEndpoint",
"glue:GetDevEndpoints",
"glue:GetJob",
"glue:GetJobBookmark",
"glue:GetJobRun",
"glue:GetJobRuns",
"glue:GetJobs",
"glue:GetMapping",
"glue:GetMLTaskRun",
"glue:GetMLTaskRuns",
"glue:GetMLTransform",
"glue:GetMLTransforms",
"glue:GetPartition",
"glue:GetPartitions",
"glue:GetPlan",
"glue:GetRegistry",
"glue:GetResourcePolicy",
"glue:GetSchema",
"glue:GetSchemaByDefinition",
"glue:GetSchemaVersion",
"glue:GetSchemaVersionsDiff",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTable",
"glue:GetTables",
"glue:GetTableVersion",
"glue:GetTableVersions",
"glue:GetTags",
"glue:GetTrigger",
"glue:GetTriggers",
"glue:GetUserDefinedFunction",
"glue:GetUserDefinedFunctions",
"glue:GetWorkflow",
"glue:GetWorkflowRun",
"glue:GetWorkflowRunProperties",
"glue:GetWorkflowRuns",
"glue:ListCrawlers",
"glue:ListCrawls",
"glue:ListDevEndpoints",
"glue:ListJobs",
"glue:ListMLTransforms",
```

```
"glue:ListRegistries",
"glue:ListSchemas",
"glue:ListSchemaVersions",
"glue:ListTriggers",
"glue:ListWorkflows",
"glue:QuerySchemaVersionMetadata",
"glue:SearchTables",
"grafana:DescribeWorkspace",
"grafana:DescribeWorkspaceAuthentication",
"grafana:DescribeWorkspaceConfiguration",
"grafana:ListPermissions",
"grafana:ListTagsForResource",
"grafana:ListVersions",
"grafana:ListWorkspaces",
"greengrass:DescribeComponent",
"greengrass:Get*",
"greengrass:List*",
"groundstation:DescribeContact",
"groundstation:GetConfig",
"groundstation:GetDataflowEndpointGroup",
"groundstation:GetMinuteUsage",
"groundstation:GetMissionProfile",
"groundstation:GetSatellite",
"groundstation:ListConfigs",
"groundstation:ListContacts",
"groundstation:ListDataflowEndpointGroups",
"groundstation:ListGroundStations",
"groundstation:ListMissionProfiles",
"groundstation:ListSatellites",
"groundstation:ListTagsForResource",
"guardduty:Describe*",
"guardduty:Get*",
"guardduty:List*",
"health:Describe*",
"healthlake:DescribeFHIRDatastore",
"healthlake:DescribeFHIRExportJob",
"healthlake:DescribeFHIRImportJob",
"healthlake:GetCapabilities",
"healthlake:ListFHIRDatastores",
"healthlake:ListFHIRExportJobs",
"healthlake:ListFHIRImportJobs",
"healthlake:ListTagsForResource",
"healthlake:ReadResource",
"healthlake:SearchWithGet",
```

```
"healthlake:SearchWithPost",
"iam:Generate*",
"iam:Get*",
"iam:List*",
"iam:Simulate*",
"identity-sync:GetSyncProfile",
"identity-sync:GetSyncTarget",
"identity-sync:ListSyncFilters",
"identitystore-auth:BatchGetSession",
"identitystore-auth:ListSessions",
"identitystore:DescribeGroup",
"identitystore:DescribeGroupMembership",
"identitystore:DescribeUser",
"identitystore:GetGroupId",
"identitystore:GetGroupMembershipId",
"identitystore:GetUserId",
"identitystore:IsMemberInGroups",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"imagebuilder:Get*",
"imagebuilder:List*",
"importexport:Get*",
"importexport:List*",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCisScans",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListMembers",
```

```
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"internetmonitor:GetHealthEvent",
"internetmonitor:GetInternetEvent",
"internetmonitor:GetMonitor",
"internetmonitor:ListHealthEvents",
"internetmonitor:ListInternetEvents",
"internetmonitor:ListMonitors",
"internetmonitor:ListTagsForResource",
" invoicing:GetInvoiceEmailDeliveryPreferences",
" invoicing:GetInvoicePDF",
" invoicing:ListInvoiceSummaries",
" iot:Describe*",
" iot:Get*",
" iot:List*",
" iot1click:DescribeDevice",
" iot1click:DescribePlacement",
" iot1click:DescribeProject",
" iot1click:GetDeviceMethods",
" iot1click:GetDevicesInPlacement",
" iot1click:ListDeviceEvents",
" iot1click:ListDevices",
" iot1click:ListPlacements",
" iot1click:ListProjects",
" iot1click:ListTagsForResource",
" iotanalytics:Describe*",
" iotanalytics:Get*",
" iotanalytics:List*",
" iotanalytics:SampleChannelData",
" iotevents:DescribeAlarm",
" iotevents:DescribeAlarmModel",
" iotevents:DescribeDetector",
" iotevents:DescribeDetectorModel",
" iotevents:DescribeInput",
" iotevents:DescribeLoggingOptions",
" iotevents:ListAlarmModels",
" iotevents:ListAlarmModelVersions",
" iotevents:ListAlarms",
" iotevents:ListDetectorModels",
" iotevents:ListDetectorModelVersions",
" iotevents:ListDetectors",
" iotevents:ListInputs",
" iotevents:ListTagsForResource",
" iotfleethub:DescribeApplication",
```

```
"iotfleethub:ListApplications",
"iotfleetwise:GetCampaign",
"iotfleetwise:GetDecoderManifest",
"iotfleetwise:GetFleet",
"iotfleetwise:GetLoggingOptions",
"iotfleetwise:GetModelManifest",
"iotfleetwise:GetRegisterAccountStatus",
"iotfleetwise:GetSignalCatalog",
"iotfleetwise:GetVehicle",
"iotfleetwise:GetVehicleStatus",
"iotfleetwise:ListCampaigns",
"iotfleetwise:ListDecoderManifestNetworkInterfaces",
"iotfleetwise:ListDecoderManifests",
"iotfleetwise:ListDecoderManifestSignals",
"iotfleetwise:ListFleets",
"iotfleetwise:ListFleetsForVehicle",
"iotfleetwise:ListModelManifestNodes",
"iotfleetwise:ListModelManifests",
"iotfleetwise:ListSignalCatalogNodes",
"iotfleetwise:ListSignalCatalogs",
"iotfleetwise:ListTagsForResource",
"iotfleetwise:ListVehicles",
"iotfleetwise:ListVehiclesInFleet",
"iotroborunner:GetDestination",
"iotroborunner:GetSite",
"iotroborunner:GetWorker",
"iotroborunner:GetWorkerFleet",
"iotroborunner:ListDestinations",
"iotroborunner:ListSites",
"iotroborunner:ListWorkerFleets",
"iotroborunner:ListWorkers",
"iotsitewise:Describe*",
"iotsitewise:Get*",
"iotsitewise:List*",
"iotwireless:GetDestination",
"iotwireless:GetDeviceProfile",
"iotwireless:GetEventConfigurationByResourceTypes",
"iotwireless:GetFuotaTask",
"iotwireless:GetLogLevelsByResourceTypes",
"iotwireless:GetMetrics",
"iotwireless:GetMetricConfiguration",
"iotwireless:GetMulticastGroup",
"iotwireless:GetMulticastGroupSession",
"iotwireless:GetNetworkAnalyzerConfiguration",
```

```
"iotwireless:GetPartnerAccount",
"iotwireless:GetPosition",
"iotwireless:GetPositionConfiguration",
"iotwireless:GetPositionEstimate",
"iotwireless:GetResourceEventConfiguration",
"iotwireless:GetResourceLogLevel",
"iotwireless:GetResourcePosition",
"iotwireless:GetServiceEndpoint",
"iotwireless:GetServiceProfile",
"iotwireless:GetWirelessDevice",
"iotwireless:GetWirelessDeviceImportTask",
"iotwireless:GetWirelessDeviceStatistics",
"iotwireless:GetWirelessGateway",
"iotwireless:GetWirelessGatewayCertificate",
"iotwireless:GetWirelessGatewayFirmwareInformation",
"iotwireless:GetWirelessGatewayStatistics",
"iotwireless:GetWirelessGatewayTask",
"iotwireless:GetWirelessGatewayTaskDefinition",
"iotwireless:ListDestinations",
"iotwireless:ListDeviceProfiles",
"iotwireless:ListDevicesForWirelessDeviceImportTask",
"iotwireless:ListEventConfigurations",
"iotwireless:ListFuotaTasks",
"iotwireless:ListMulticastGroups",
"iotwireless:ListMulticastGroupsByFuotaTask",
"iotwireless:ListNetworkAnalyzerConfigurations",
"iotwireless:ListPartnerAccounts",
"iotwireless:ListPositionConfigurations",
"iotwireless:ListQueuedMessages",
"iotwireless:ListServiceProfiles",
"iotwireless:ListTagsForResource",
"iotwireless:ListWirelessDeviceImportTasks",
"iotwireless:ListWirelessDevices",
"iotwireless:ListWirelessGateways",
"iotwireless:ListWirelessGatewayTaskDefinitions",
"ivs:BatchGetChannel",
"ivs:GetChannel",
"ivs:GetComposition",
"ivs:GetEncoderConfiguration",
"ivs:GetStage",
"ivs:GetStageSession",
"ivs:GetParticipant",
"ivs:GetPlaybackKeyPair",
"ivs:GetPlaybackRestrictionPolicy",
```

```
"ivs:GetRecordingConfiguration",
"ivs:GetStreamSession",
"ivs:ListChannels",
"ivs:ListCompositions",
"ivs:ListEncoderConfigurations",
"ivs:ListParticipants",
"ivs:ListParticipantEvents",
"ivs:ListPlaybackKeyPairs",
"ivs:ListPlaybackRestrictionPolicies",
"ivs:ListRecordingConfigurations",
"ivs:ListStages",
"ivs:ListStageSessions",
"ivs:ListStreams",
"ivs:ListStreamKeys",
"ivs:ListStreamSessions",
"ivs:ListTagsForResource",
"ivschat:GetLoggingConfiguration",
"ivschat:GetRoom",
"ivschat:ListLoggingConfigurations",
"ivschat:ListRooms",
"ivschat:ListTagsForResource",
"kafka:Describe*",
"kafka:DescribeCluster",
"kafka:DescribeClusterOperation",
"kafka:DescribeClusterV2",
"kafka:DescribeConfiguration",
"kafka:DescribeConfigurationRevision",
"kafka:Get*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafka:ListClusterOperations",
"kafka:ListClusters",
"kafka:ListClustersV2",
"kafka:ListConfigurationRevisions",
"kafka:ListConfigurations",
"kafka:ListKafkaVersions",
"kafka:ListNodes",
"kafka:ListTagsForResource",
"kafkaconnect:DescribeConnector",
"kafkaconnect:DescribeCustomPlugin",
"kafkaconnect:DescribeWorkerConfiguration",
"kafkaconnect:ListConnectors",
"kafkaconnect:ListCustomPlugins",
```

```
"kafkaconnect:ListWorkerConfigurations",
"kendra:BatchGetDocumentStatus",
"kendra:DescribeDataSource",
"kendra:DescribeExperience",
"kendra:DescribeFaq",
"kendra:DescribeIndex",
"kendra:DescribePrincipalMapping",
"kendra:DescribeQuerySuggestionsBlockList",
"kendra:DescribeQuerySuggestionsConfig",
"kendra:DescribeThesaurus",
"kendra:GetQuerySuggestions",
"kendra:GetSnapshots",
"kendra:ListDataSources",
"kendra:ListDataSourceSyncJobs",
"kendra:ListEntityPersonas",
"kendra:ListExperienceEntities",
"kendra:ListExperiences",
"kendra:ListFaqs",
"kendra:ListGroupsOlderThanOrderingId",
"kendra:ListIndices",
"kendra:ListQuerySuggestionsBlockLists",
"kendra:ListTagsForResource",
"kendra:ListThesauri",
"kendra:Query",
"kinesis:Describe*",
"kinesis:Get*",
"kinesis:List*",
"kinesisanalytics:Describe*",
"kinesisanalytics:Discover*",
"kinesisanalytics:Get*",
"kinesisanalytics:List*",
"kinesisvideo:Describe*",
"kinesisvideo:Get*",
"kinesisvideo:List*",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lakeformation:DescribeResource",
"lakeformation:GetDataCellsFilter",
"lakeformation:GetDataLakeSettings",
"lakeformation:GetEffectivePermissionsForPath",
"lakeformation:GetLfTag",
"lakeformation:GetResourceLfTags",
"lakeformation:ListDataCellsFilter",
```



```
"lakeformation:ListLfTags",
"lakeformation:ListPermissions",
"lakeformation:ListResources",
"lakeformation:ListTableStorageOptimizers",
"lakeformation:SearchDatabasesByLfTags",
"lakeformation:SearchTablesByLfTags",
"lambda:Get*",
"lambda:List*",
"launchwizard:DescribeAdditionalNode",
"launchwizard:DescribeProvisionedApp",
"launchwizard:DescribeProvisioningEvents",
"launchwizard:DescribeSettingsSet",
"launchwizard:GetDeployment",
"launchwizard:GetInfrastructureSuggestion",
"launchwizard:GetIpAddress",
"launchwizard:GetResourceCostEstimate",
"launchwizard:GetResourceRecommendation",
"launchwizard:GetSettingsSet",
"launchwizard:GetWorkload",
"launchwizard:GetWorkloadAsset",
"launchwizard:GetWorkloadAssets",
"launchwizard:ListAdditionalNodes",
"launchwizard:ListAllowedResources",
"launchwizard:ListDeploymentEvents",
"launchwizard:ListDeployments",
"launchwizard:ListProvisionedApps",
"launchwizard:ListResourceCostEstimates",
"launchwizard:ListSettingsSets",
"launchwizard:ListWorkloadDeploymentOptions",
"launchwizard:ListWorkloadDeploymentPatterns",
"launchwizard:ListWorkloads",
"lex:DescribeBot",
"lex:DescribeBotAlias",
"lex:DescribeBotChannel",
"lex:DescribeBotLocale",
"lex:DescribeBotVersion",
"lex:DescribeExport",
"lex:DescribeImport",
"lex:DescribeIntent",
"lex:DescribeResourcePolicy",
"lex:DescribeSlot",
"lex:DescribeSlotType",
"lex:Get*",
"lex:ListBotAliases",
```

```
"lex:ListBotChannels",
"lex:ListBotLocales",
"lex:ListBots",
"lex:ListBotVersions",
"lex:ListBuiltInIntents",
"lex:ListBuiltInSlotTypes",
"lex:ListExports",
"lex:ListImports",
"lex:ListIntents",
"lex:ListSlots",
"lex:ListSlotTypes",
"lex:ListTagsForResource",
"license-manager:Get*",
"license-manager:List*",
"lightsail:GetActiveNames",
"lightsail:GetAlarms",
"lightsail:GetAutoSnapshots",
"lightsail:GetBlueprints",
"lightsail:GetBucketAccessKeys",
"lightsail:GetBucketBundles",
"lightsail:GetBucketMetricData",
"lightsail:GetBuckets",
"lightsail:GetBundles",
"lightsail:GetCertificates",
"lightsail:GetCloudFormationStackRecords",
"lightsail:GetContainerAPIMetadata",
"lightsail:GetContainerImages",
"lightsail:GetContainerServiceDeployments",
"lightsail:GetContainerServiceMetricData",
"lightsail:GetContainerServicePowers",
"lightsail:GetContainerServices",
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshot",
"lightsail:GetDiskSnapshots",
"lightsail:GetDistributionBundles",
"lightsail:GetDistributionLatestCacheReset",
"lightsail:GetDistributionMetricData",
"lightsail:GetDistributions",
"lightsail:GetDomain",
"lightsail:GetDomains",
"lightsail:GetExportSnapshotRecords",
"lightsail:GetInstance",
"lightsail:GetInstanceMetricData",
```

```
"lightsail:GetInstancePortStates",
"lightsail:GetInstances",
"lightsail:GetInstanceSnapshot",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstanceState",
"lightsail:GetKeyPair",
"lightsail:GetKeyPairs",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancerMetricData",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetOperation",
"lightsail:GetOperations",
"lightsail:GetOperationsForResource",
"lightsail:GetRegions",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseBlueprints",
"lightsail:GetRelationalDatabaseBundles",
"lightsail:GetRelationalDatabaseEvents",
"lightsail:GetRelationalDatabaseLogEvents",
"lightsail:GetRelationalDatabaseLogStreams",
"lightsail:GetRelationalDatabaseMetricData",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetRelationalDatabaseSnapshot",
"lightsail:GetRelationalDatabaseSnapshots",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"lightsail:Is*",
"logs:Describe*",
"logs:FilterLogEvents",
"logs:Get*",
"logs:ListAnomalies",
"logs:ListLogAnomalyDetectors",
"logs:ListLogDeliveries",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"logs:StartLiveTail",
"logs:StartQuery",
"logs:StopLiveTail",
"logs:StopQuery",
"logs:TestMetricFilter",
"lookoutequipment:DescribeDataIngestionJob",
"lookoutequipment:DescribeDataset",
```

```
"lookoutequipment:DescribeInferenceScheduler",
"lookoutequipment:DescribeLabel",
"lookoutequipment:DescribeLabelGroup",
"lookoutequipment:DescribeModel",
"lookoutequipment:DescribeModelVersion",
"lookoutequipment:DescribeResourcePolicy",
"lookoutequipment:DescribeRetrainingScheduler",
"lookoutequipment:ListDataIngestionJobs",
"lookoutequipment:ListDatasets",
"lookoutequipment:ListInferenceEvents",
"lookoutequipment:ListInferenceExecutions",
"lookoutequipment:ListInferenceSchedulers",
"lookoutequipment:ListLabelGroups",
"lookoutequipment:ListLabels",
"lookoutequipment:ListModels",
"lookoutequipment:ListModelVersions",
"lookoutequipment:ListRetrainingSchedulers",
"lookoutequipment:ListSensorStatistics",
"lookoutequipment:ListTagsForResource",
"lookoutmetrics:Describe*",
"lookoutmetrics:Get*",
"lookoutmetrics:List*",
"lookoutvision:DescribeDataset",
"lookoutvision:DescribeModel",
"lookoutvision:DescribeModelPackagingJob",
"lookoutvision:DescribeProject",
"lookoutvision:ListDatasetEntries",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"lookoutvision:ListTagsForResource",
"m2:GetApplication",
"m2:GetApplicationVersion",
"m2:GetBatchJobExecution",
"m2:GetDataSetDetails",
"m2:GetDataSetImportTask",
"m2:GetDeployment",
"m2:GetEnvironment",
"m2:ListApplications",
"m2:ListApplicationVersions",
"m2:ListBatchJobDefinitions",
"m2:ListBatchJobExecutions",
"m2:ListDataSetImportHistory",
"m2:ListDataSets",
```

```
"m2:ListDeployments",
"m2:ListEngineVersions",
"m2:ListEnvironments",
"m2:ListTagsForResource",
"machinelearning:Describe*",
"machinelearning:Get*",
"macie2:BatchGetCustomDataIdentifiers",
"macie2:DescribeBuckets",
"macie2:DescribeClassificationJob",
"macie2:DescribeOrganizationConfiguration",
"macie2:GetAdministratorAccount",
"macie2:GetAllowList",
"macie2:GetAutomatedDiscoveryConfiguration",
"macie2:GetBucketStatistics",
"macie2:GetClassificationExportConfiguration",
"macie2:GetClassificationScope",
"macie2:GetCustomDataIdentifier",
"macie2:GetFindings",
"macie2:GetFindingsFilter",
"macie2:GetFindingsPublicationConfiguration",
"macie2:GetFindingStatistics",
"macie2:GetInvitationsCount",
"macie2:GetMacieSession",
"macie2:GetMember",
"macie2:GetResourceProfile",
"macie2:GetRevealConfiguration",
"macie2:GetSensitiveDataOccurrencesAvailability",
"macie2:GetSensitivityInspectionTemplate",
"macie2:GetUsageStatistics",
"macie2:GetUsageTotals",
"macie2:ListAllowLists",
"macie2:ListClassificationJobs",
"macie2:ListClassificationScopes",
"macie2:ListCustomDataIdentifiers",
"macie2:ListFindings",
"macie2:ListFindingsFilters",
"macie2:ListInvitations",
"macie2:ListMembers",
"macie2:ListOrganizationAdminAccounts",
"macie2:ListResourceProfileArtifacts",
"macie2:ListResourceProfileDetections",
"macie2:ListSensitivityInspectionTemplates",
"macie2:ListTagsForResource",
"macie2:SearchResources",
```

```
"managedblockchain:GetMember",
"managedblockchain:GetNetwork",
"managedblockchain:GetNode",
"managedblockchain:GetProposal",
"managedblockchain:ListInvitations",
"managedblockchain:ListMembers",
"managedblockchain:ListNetworks",
"managedblockchain:ListNodes",
"managedblockchain:ListProposals",
"managedblockchain:ListProposalVotes",
"managedblockchain:ListTagsForResource",
"mediaconnect:DescribeFlow",
"mediaconnect:DescribeOffering",
"mediaconnect:DescribeReservation",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mediaconnect:ListTagsForResource",
"mediaconvert:DescribeEndpoints",
"mediaconvert:Get*",
"mediaconvert:List*",
"medialive:DescribeChannel",
"medialive:DescribeInput",
"medialive:DescribeInputDevice",
"medialive:DescribeInputDeviceThumbnail",
"medialive:DescribeInputSecurityGroup",
"medialive:DescribeMultiplex",
"medialive:DescribeMultiplexProgram",
"medialive:DescribeOffering",
"medialive:DescribeReservation",
"medialive:DescribeSchedule",
"medialive:GetCloudWatchAlarmTemplate",
"medialive:GetCloudWatchAlarmTemplateGroup",
"medialive:GetEventBridgeRuleTemplate",
"medialive:GetEventBridgeRuleTemplateGroup",
"medialive:GetSignalMap",
"medialive:ListChannels",
"medialive:ListCloudWatchAlarmTemplateGroups",
"medialive:ListCloudWatchAlarmTemplates",
"medialive:ListEventBridgeRuleTemplateGroups",
"medialive:ListEventBridgeRuleTemplates",
"medialive:ListInputDevices",
"medialive:ListInputDeviceTransfers",
```

```
"medialive:ListInputs",
"medialive:ListInputSecurityGroups",
"medialive:ListMultiplexes",
"medialive:ListMultiplexPrograms",
"medialive:ListOfferings",
"medialive:ListReservations",
"medialive:ListSignalMaps",
"medialive:ListTagsForResource",
"mediapackage-vod:Describe*",
"mediapackage-vod:List*",
"mediapackage:Describe*",
"mediapackage:List*",
"mediapackagev2:GetChannel",
"mediapackagev2:GetChannelGroup",
"mediapackagev2:GetChannelPolicy",
"mediapackagev2:GetHeadObject",
"mediapackagev2:GetObject",
"mediapackagev2:GetOriginEndpoint",
"mediapackagev2:GetOriginEndpointPolicy",
"mediapackagev2:ListChannelGroups",
"mediapackagev2:ListChannels",
"mediapackagev2:ListOriginEndpoints",
"mediapackagev2:ListTagsForResource",
"mediastore:DescribeContainer",
"mediastore:DescribeObject",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:GetLifecyclePolicy",
"mediastore:GetMetricPolicy",
"mediastore:GetObject",
"mediastore:ListContainers",
"mediastore:ListItems",
"mediastore:ListTagsForResource",
"memorydb:DescribeClusters",
"memorydb:DescribeParameterGroups",
"memorydb:DescribeParameters",
"memorydb:ListTags",
"mgh:Describe*",
"mgh:GetHomeRegion",
"mgh:List*",
"mgn:DescribeJobLogItems",
"mgn:DescribeJobs",
"mgn:DescribeLaunchConfigurationTemplates",
"mgn:DescribeReplicationConfigurationTemplates",
```

```
"mgn:DescribeSourceServers",
"mgn:DescribeVcenterClients",
"mgn:GetLaunchConfiguration",
"mgn:GetReplicationConfiguration",
"mgn:ListApplications",
"mgn:ListSourceServerActions",
"mgn:ListTemplateActions",
"mgn:ListWaves",
"mobileanalytics:Get*",
"mobiletargeting:Get*",
"mobiletargeting:List*",
"monitron:GetProject",
"monitron:GetProjectAdminUser",
"monitron:ListProjects",
"monitron:ListTagsForResource",
"mq:Describe*",
"mq:List*",
"network-firewall:DescribeFirewall",
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:DescribeRuleGroupMetadata",
"network-firewall:DescribeTLSInspectionConfiguration",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"network-firewall:ListTagsForResource",
"network-firewall:ListTLSInspectionConfigurations",
"networkmanager:DescribeGlobalNetworks",
"networkmanager:GetConnectAttachment",
"networkmanager:GetConnections",
"networkmanager:GetConnectPeer",
"networkmanager:GetConnectPeerAssociations",
"networkmanager:GetCoreNetwork",
"networkmanager:GetCoreNetworkChangeEvents",
"networkmanager:GetCoreNetworkChangeSet",
"networkmanager:GetCoreNetworkPolicy",
"networkmanager:GetCustomerGatewayAssociations",
"networkmanager:GetDevices",
"networkmanager:GetLinkAssociations",
"networkmanager:GetLinks",
"networkmanager:GetNetworkResourceCounts",
"networkmanager:GetNetworkResourceRelationships",
```



```
"networkmanager:GetNetworkResources",
"networkmanager:GetNetworkRoutes",
"networkmanager:GetNetworkTelemetry",
"networkmanager:GetResourcePolicy",
"networkmanager:GetRouteAnalysis",
"networkmanager:GetSites",
"networkmanager:GetSiteToSiteVpnAttachment",
"networkmanager:GetTransitGatewayConnectPeerAssociations",
"networkmanager:GetTransitGatewayPeering",
"networkmanager:GetTransitGatewayRegistrations",
"networkmanager:GetTransitGatewayRouteTableAttachment",
"networkmanager:GetVpcAttachment",
"networkmanager:ListAttachments",
"networkmanager:ListConnectPeers",
"networkmanager:ListCoreNetworkPolicyVersions",
"networkmanager:ListCoreNetworks",
"networkmanager:ListPeerings",
"networkmanager:ListTagsForResource",
"nimble:GetEula",
"nimble:GetFeatureMap",
"nimble:GetLaunchProfile",
"nimble:GetLaunchProfileDetails",
"nimble:GetLaunchProfileInitialization",
"nimble:GetLaunchProfileMember",
"nimble:GetStreamingImage",
"nimble:GetStreamingSession",
"nimble:GetStudio",
"nimble:GetStudioComponent",
"nimble:GetStudioMember",
"nimble:ListEulaAcceptances",
"nimble:ListEulas",
"nimble:ListLaunchProfileMembers",
"nimble:ListLaunchProfiles",
"nimble:ListStreamingImages",
"nimble:ListStreamingSessions",
"nimble:ListStudioComponents",
"nimble:ListStudioMembers",
"nimble:ListStudios",
"nimble:ListTagsForResource",
"notifications-contacts:GetEmailContact",
"notifications-contacts:ListEmailContacts",
"notifications-contacts:ListTagsForResource",
"notifications:GetEventRule",
"notifications:GetNotificationConfiguration",
```

```
"notifications:GetNotificationEvent",
"notifications:ListChannels",
"notifications:ListEventRules",
"notifications:ListNotificationConfigurations",
"notifications:ListNotificationEvents",
"notifications:ListNotificationHubs",
"notifications:ListTagsForResource",
"oam:GetLink",
"oam:GetSink",
"oam:GetSinkPolicy",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"omics:Get*",
"omics:List*",
"one:GetDeviceConfigurationTemplate",
"one:GetDeviceInstance",
"one:GetDeviceInstanceConfiguration",
"one:GetSite",
"one:GetSiteAddress",
"one:ListDeviceConfigurationTemplates",
"one:ListDeviceInstances",
"one:ListSites",
"one:ListUsers",
"opsworks-cm:Describe*",
"opsworks-cm:List*",
"opsworks:Describe*",
"opsworks:Get*",
"organizations:Describe*",
"organizations:List*",
"osis:GetPipeline",
"osis:GetPipelineBlueprint",
"osis:GetPipelineChangeProgress",
"osis:ListPipelineBlueprints",
"osis:ListPipelines",
"osis:ListTagsForResource",
"outposts:Get*",
"outposts:List*",
"payment-cryptography:GetAlias",
"payment-cryptography:GetKey",
"payment-cryptography:GetPublicKeyCertificate",
"payment-cryptography:ListAliases",
"payment-cryptography:ListKeys",
"payment-cryptography:ListTagsForResource",
```

```
"payments:GetPaymentInstrument",
"payments:GetPaymentStatus",
"payments:ListPaymentPreferences",
"pca-connector-ad:GetConnector",
"pca-connector-ad:GetDirectoryRegistration",
"pca-connector-ad:GetServicePrincipalName",
"pca-connector-ad:GetTemplate",
"pca-connector-ad:GetTemplateGroupAccessControlEntry",
"pca-connector-ad:ListConnectors",
"pca-connector-ad:ListDirectoryRegistrations",
"pca-connector-ad:ListServicePrincipalNames",
"pca-connector-ad:ListTagsForResource",
"pca-connector-ad:ListTemplateGroupAccessControlEntries",
"pca-connector-ad:ListTemplates",
"personalize:Describe*",
"personalize:Get*",
"personalize:List*",
"pi:DescribeDimensionKeys",
"pi:GetDimensionKeyDetails",
"pi:GetResourceMetadata",
"pi:GetResourceMetrics",
"pi:ListAvailableResourceDimensions",
"pi:ListAvailableResourceMetrics",
"pipes:DescribePipe",
"pipes:ListPipes",
"pipes:ListTagsForResource",
"polly:Describe*",
"polly:Get*",
"polly:List*",
"polly:SynthesizeSpeech",
"pricing:DescribeServices",
"pricing:GetAttributeValues",
"pricing:GetPriceListFileUrl",
"pricing:GetProducts",
"pricing:ListPriceLists",
"proton:GetDeployment",
"proton:GetEnvironment",
"proton:GetEnvironmentTemplate",
"proton:GetEnvironmentTemplateVersion",
"proton:GetService",
"proton:GetServiceInstance",
"proton:GetServiceTemplate",
"proton:GetServiceTemplateVersion",
"proton:ListDeployments",
```

```
"proton:ListEnvironmentAccountConnections",
"proton:ListEnvironments",
"proton:ListEnvironmentTemplates",
"proton:ListServiceInstances",
"proton:ListServices",
"proton:ListServiceTemplates",
"proton:ListTagsForResource",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:ListPurchaseOrderInvoices",
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ViewPurchaseOrders",
"qldb:DescribeJournalKinesisStream",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:GetBlock",
"qldb:GetDigest",
"qldb:GetRevision",
"qldb:ListJournalKinesisStreamsForLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"qldb:ListTagsForResource",
"ram:Get*",
"ram:List*",
"rbin:GetRule",
"rbin:ListRules",
"rbin:ListTagsForResource",
"rds:Describe*",
"rds:Download*",
"rds:List*",
"redshift-serverless:GetCustomDomainAssociation",
"redshift-serverless:GetEndpointAccess",
"redshift-serverless:GetNamespace",
"redshift-serverless:GetRecoveryPoint",
"redshift-serverless:GetResourcePolicy",
"redshift-serverless:GetScheduledAction",
"redshift-serverless:GetSnapshot",
"redshift-serverless:GetTableRestoreStatus",
"redshift-serverless:GetUsageLimit",
"redshift-serverless:GetWorkgroup",
"redshift-serverless:ListCustomDomainAssociations",
"redshift-serverless:ListEndpointAccess",
"redshift-serverless:ListNamespaces",
"redshift-serverless:ListRecoveryPoints",
```

```
"redshift-serverless:ListScheduledActions",
"redshift-serverless:ListSnapshotCopyConfigurations",
"redshift-serverless:ListSnapshots",
"redshift-serverless:ListTableRestoreStatus",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListUsageLimits",
"redshift-serverless:ListWorkgroups",
"redshift:Describe*",
"redshift:GetReservedNodeExchangeOfferings",
"redshift:ListRecommendations",
"redshift:View*",
"refactor-spaces:GetApplication",
"refactor-spaces:GetEnvironment",
"refactor-spaces:GetResourcePolicy",
"refactor-spaces:GetRoute",
"refactor-spaces:GetService",
"refactor-spaces:ListApplications",
"refactor-spaces:ListEnvironments",
"refactor-spaces:ListEnvironmentVpcs",
"refactor-spaces:ListRoutes",
"refactor-spaces:ListServices",
"refactor-spaces:ListTagsForResource",
"rekognition:CompareFaces",
"rekognition:DescribeDataset",
"rekognition:DescribeProjects",
"rekognition:DescribeProjectVersions",
"rekognition:DescribeStreamProcessor",
"rekognition:Detect*",
"rekognition:GetCelebrityInfo",
"rekognition:GetCelebrityRecognition",
"rekognition:GetContentModeration",
"rekognition:GetFaceDetection",
"rekognition:GetFaceSearch",
"rekognition:GetLabelDetection",
"rekognition:GetPersonTracking",
"rekognition:GetSegmentDetection",
"rekognition:GetTextDetection",
"rekognition:List*",
"rekognition:RecognizeCelebrities",
"rekognition:Search*",
"resiliencehub:DescribeApp",
"resiliencehub:DescribeAppAssessment",
"resiliencehub:DescribeAppVersion",
"resiliencehub:DescribeAppVersionAppComponent",
```

```
"resiliencehub:DescribeAppVersionResource",
"resiliencehub:DescribeAppVersionResourcesResolutionStatus",
"resiliencehub:DescribeAppVersionTemplate",
"resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
"resiliencehub:DescribeResiliencyPolicy",
"resiliencehub:ListAlarmRecommendations",
"resiliencehub:ListAppAssessmentComplianceDrifts",
"resiliencehub:ListAppAssessments",
"resiliencehub:ListAppComponentCompliances",
"resiliencehub:ListAppComponentRecommendations",
"resiliencehub:ListAppInputSources",
"resiliencehub:ListApps",
"resiliencehub:ListAppVersionAppComponents",
"resiliencehub:ListAppVersionResourceMappings",
"resiliencehub:ListAppVersionResources",
"resiliencehub:ListAppVersions",
"resiliencehub:ListRecommendationTemplates",
"resiliencehub:ListResiliencyPolicies",
"resiliencehub:ListSopRecommendations",
"resiliencehub:ListSuggestedResiliencyPolicies",
"resiliencehub:ListTagsForResource",
"resiliencehub:ListTestRecommendations",
"resiliencehub:ListUnsupportedAppVersionResources",
"resource-explorer-2:BatchGetView",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:GetView",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"resource-explorer-2:Search",
"resource-groups:Get*",
"resource-groups:List*",
"resource-groups:Search*",
"robomaker:BatchDescribe*",
"robomaker:Describe*",
"robomaker:Get*",
"robomaker:List*",
"route53-recovery-cluster:Get*",
"route53-recovery-cluster:ListRoutingControls",
"route53-recovery-control-config:Describe*",
"route53-recovery-control-config:GetResourcePolicy",
"route53-recovery-control-config:List*",
```

```
"route53-recovery-readiness:Get*",
"route53-recovery-readiness:List*",
"route53:Get*",
"route53:List*",
"route53:Test*",
"route53domains:Check*",
"route53domains:Get*",
"route53domains:List*",
"route53domains:View*",
"route53profiles:GetProfile",
"route53profiles:GetProfileAssociation",
"route53profiles:GetProfileResourceAssociation",
"route53profiles:ListProfileAssociations",
"route53profiles:ListProfileResourceAssociations",
"route53profiles:ListProfiles",
"route53profiles:ListTagsForResource",
"route53resolver:Get*",
"route53resolver:List*",
"rum:GetAppMonitor",
"rum:GetAppMonitorData",
"rum:ListAppMonitors",
"s3-object-lambda:GetObject",
"s3-object-lambda:GetObjectAcl",
"s3-object-lambda:GetObjectLegalHold",
"s3-object-lambda:GetObjectRetention",
"s3-object-lambda:GetObjectTagging",
"s3-object-lambda:GetObjectVersion",
"s3-object-lambda:GetObjectVersionAcl",
"s3-object-lambda:GetObjectVersionTagging",
"s3-object-lambda:ListBucket",
"s3-object-lambda:ListBucketMultipartUploads",
"s3-object-lambda:ListBucketVersions",
"s3-object-lambda:ListMultipartUploadParts",
"s3:DescribeJob",
"s3:Get*",
"s3:List*",
"sagemaker-groundtruth-synthetic:GetAccountDetails",
"sagemaker-groundtruth-synthetic:GetBatch",
"sagemaker-groundtruth-synthetic:GetProject",
"sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
"sagemaker-groundtruth-synthetic:ListBatchSummaries",
"sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
"sagemaker-groundtruth-synthetic:ListProjectSummaries",
"sagemaker:Describe*",
```

```
"sagemaker:GetSearchSuggestions",
"sagemaker:List*",
"sagemaker:Search",
"savingsplans:DescribeSavingsPlanRates",
"savingsplans:DescribeSavingsPlans",
"savingsplans:DescribeSavingsPlansOfferingRates",
"savingsplans:DescribeSavingsPlansOfferings",
"savingsplans:ListTagsForResource",
"scheduler:GetSchedule",
"scheduler:GetScheduleGroup",
"scheduler:ListScheduleGroups",
"scheduler:ListSchedules",
"scheduler:ListTagsForResource",
"schemas:Describe*",
"schemas:Get*",
"schemas:List*",
"schemas:Search*",
"sdb:Get*",
"sdb:List*",
"sdb:Select*",
"secretsmanager:Describe*",
"secretsmanager:GetResourcePolicy",
"secretsmanager:List*",
"securityhub:BatchGetControlEvaluations",
"securityhub:BatchGetSecurityControls",
"securityhub:BatchGetStandardsControlAssociations",
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"securitylake:GetDataLakeExceptionSubscription",
"securitylake:GetDataLakeOrganizationConfiguration",
"securitylake:GetDataLakeSources",
"securitylake:GetSubscriber",
"securitylake:ListDataLakeExceptions",
"securitylake:ListDataLakes",
"securitylake:ListLogSources",
"securitylake:ListSubscribers",
"securitylake:ListTagsForResource",
"serverlessrepo:Get*",
"serverlessrepo:List*",
"serverlessrepo:SearchApplications",
"servicecatalog:Describe*",
"servicecatalog:GetApplication",
"servicecatalog:GetAttributeGroup",
```



```
"servicecatalog:List*",
"servicecatalog:Scan*",
"servicecatalog:Search*",
"servicediscovery:DiscoverInstances",
"servicediscovery:DiscoverInstancesRevision",
"servicediscovery:Get*",
"servicediscovery:List*",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"ses:BatchGetMetricData",
"ses:Describe*",
"ses:Get*",
"ses:List*",
"shield:Describe*",
"shield:Get*",
"shield:List*",
"signer:DescribeSigningJob",
"signer:GetSigningPlatform",
"signer:GetSigningProfile",
"signer:ListProfilePermissions",
"signer:ListSigningJobs",
"signer:ListSigningPlatforms",
"signer:ListSigningProfiles",
"signer:ListTagsForResource",
"signin:ListTrustedIdentityPropagationApplicationsForConsole",
"sms-voice:DescribeAccountAttributes",
"sms-voice:DescribeAccountLimits",
"sms-voice:DescribeConfigurationSets",
"sms-voice:DescribeKeywords",
"sms-voice:DescribeOptedOutNumbers",
"sms-voice:DescribeOptOutLists",
"sms-voice:DescribePhoneNumbers",
"sms-voice:DescribePools",
"sms-voice:DescribeSenderId",
"sms-voice:DescribeSpendLimits",
```

```
"sms-voice:ListPoolOriginationIdentities",
"sms-voice:ListTagsForResource",
"snowball:Describe*",
"snowball:Get*",
"snowball:List*",
"sns:Check*",
"sns:Get*",
"sns:List*",
"sqs:Get*",
"sqs:List*",
"sqs:Receive*",
"ssm-contacts:DescribeEngagement",
"ssm-contacts:DescribePage",
"ssm-contacts:GetContact",
"ssm-contacts:GetContactChannel",
"ssm-contacts:ListContactChannels",
"ssm-contacts:ListContacts",
"ssm-contacts:ListEngagements",
"ssm-contacts:ListPageReceipts",
"ssm-contacts:ListPagesByContact",
"ssm-contacts:ListPagesByEngagement",
"ssm-incidents:GetIncidentRecord",
"ssm-incidents:GetReplicationSet",
"ssm-incidents:GetResourcePolicies",
"ssm-incidents:GetResponsePlan",
"ssm-incidents:GetTimelineEvent",
"ssm-incidents:ListIncidentRecords",
"ssm-incidents:ListRelatedItems",
"ssm-incidents:ListReplicationSets",
"ssm-incidents:ListResponsePlans",
"ssm-incidents:ListTagsForResource",
"ssm-incidents:ListTimelineEvents",
"ssm:Describe*",
"ssm:Get*",
"ssm:List*",
"sso-directory:Describe*",
"sso-directory:List*",
"sso-directory:Search*",
"sso:Describe*",
"sso:Get*",
"sso:List*",
"sso:Search*",
"states:Describe*",
"states:GetExecutionHistory",
```

```
"states:List*",
"states:ValidateStateMachineDefinition",
"storagegateway:Describe*",
"storagegateway:List*",
"sts:GetAccessKeyInfo",
"sts:GetCallerIdentity",
"sts:GetSessionToken",
"support:DescribeAttachment",
"support:DescribeCases",
"support:DescribeCommunications",
"support:DescribeServices",
"support:DescribeSeverityLevels",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
"support:DescribeTrustedAdvisorCheckResult",
"support:DescribeTrustedAdvisorChecks",
"support:DescribeTrustedAdvisorCheckSummaries",
"supportplans:GetSupportPlan",
"supportplans:GetSupportPlanUpdateStatus",
"sustainability:GetCarbonFootprintSummary",
"swf:Count*",
"swf:Describe*",
"swf:Get*",
"swf:List*",
"synthetics:Describe*",
"synthetics:Get*",
"synthetics:List*",
>tag:DescribeReportCreation",
>tag:Get*",
"tax:GetExemptions",
"tax:GetTaxInheritance",
"tax:GetTaxInterview",
"tax:GetTaxRegistration",
"tax:GetTaxRegistrationDocument",
"tax:ListTaxRegistrations",
"timestream:DescribeBatchLoadTask",
"timestream:DescribeDatabase",
"timestream:DescribeEndpoints",
"timestream:DescribeTable",
"timestream:ListBatchLoadTasks",
"timestream:ListDatabases",
"timestream:ListMeasures",
"timestream:ListTables",
"timestream:ListTagsForResource",
"tnb:GetSolFunctionInstance",
```

```
"tnb:GetSolFunctionPackage",
"tnb:GetSolFunctionPackageContent",
"tnb:GetSolFunctionPackageDescriptor",
"tnb:GetSolNetworkInstance",
"tnb:GetSolNetworkOperation",
"tnb:GetSolNetworkPackage",
"tnb:GetSolNetworkPackageContent",
"tnb:GetSolNetworkPackageDescriptor",
"tnb:ListSolFunctionInstances",
"tnb:ListSolFunctionPackages",
"tnb:ListSolNetworkInstances",
"tnb:ListSolNetworkOperations",
"tnb:ListSolNetworkPackages",
"tnb:ListTagsForResource",
"transcribe:Get*",
"transcribe:List*",
"transfer:Describe*",
"transfer:List*",
"transfer:TestIdentityProvider",
"translate:DescribeTextTranslationJob",
"translate:GetParallelData",
"translate:GetTerminology",
"translate:ListParallelData",
"translate:ListTerminologies",
"translate:ListTextTranslationJobs",
"trustedadvisor:Describe*",
"verifiedpermissions:GetIdentitySource",
"verifiedpermissions:GetPolicy",
"verifiedpermissions:GetPolicyStore",
"verifiedpermissions:GetPolicyTemplate",
"verifiedpermissions:GetSchema",
"verifiedpermissions:IsAuthorized",
"verifiedpermissions:IsAuthorizedWithToken",
"verifiedpermissions:ListIdentitySources",
"verifiedpermissions:ListPolicies",
"verifiedpermissions:ListPolicyStores",
"verifiedpermissions:ListPolicyTemplates",
"vpc-lattice:GetAccessLogSubscription",
"vpc-lattice:GetAuthPolicy",
"vpc-lattice:GetListener",
"vpc-lattice:GetResourcePolicy",
"vpc-lattice:GetRule",
"vpc-lattice:GetService",
"vpc-lattice:GetServiceNetwork",
```

```
"vpc-lattice:GetServiceNetworkServiceAssociation",
"vpc-lattice:GetServiceNetworkVpcAssociation",
"vpc-lattice:GetTargetGroup",
"vpc-lattice:ListAccessLogSubscriptions",
"vpc-lattice:ListListeners",
"vpc-lattice:ListRules",
"vpc-lattice:ListServiceNetworks",
"vpc-lattice:ListServiceNetworkServiceAssociations",
"vpc-lattice:ListServiceNetworkVpcAssociations",
"vpc-lattice:ListServices",
"vpc-lattice:ListTagsForResource",
"vpc-lattice:ListTargetGroups",
"vpc-lattice:ListTargets",
"waf-regional:Get*",
"waf-regional:List*",
"waf:Get*",
"waf:List*",
"wafv2:CheckCapacity",
"wafv2:Describe*",
"wafv2:Get*",
"wafv2:List*",
"wellarchitected:ExportLens",
"wellarchitected:GetAnswer",
"wellarchitected:GetConsolidatedReport",
"wellarchitected:GetLens",
"wellarchitected:GetLensReview",
"wellarchitected:GetLensReviewReport",
"wellarchitected:GetLensVersionDifference",
"wellarchitected:GetMilestone",
"wellarchitected:GetProfile",
"wellarchitected:GetProfileTemplate",
"wellarchitected:GetReviewTemplate",
"wellarchitected:GetReviewTemplateAnswer",
"wellarchitected:GetReviewTemplateLensReview",
"wellarchitected:GetWorkload",
"wellarchitected:ListAnswers",
"wellarchitected:ListCheckDetails",
"wellarchitected:ListCheckSummaries",
"wellarchitected:ListLenses",
"wellarchitected:ListLensReviewImprovements",
"wellarchitected:ListLensReviews",
"wellarchitected:ListLensShares",
"wellarchitected:ListMilestones",
"wellarchitected:ListNotifications",
```

```
"wellarchitected:ListProfileNotifications",
"wellarchitected:ListProfiles",
"wellarchitected:ListProfileShares",
"wellarchitected:ListReviewTemplateAnswers",
"wellarchitected:ListReviewTemplates",
"wellarchitected:ListShareInvitations",
"wellarchitected:ListTagsForResource",
"wellarchitected:ListTemplateShares",
"wellarchitected:ListWorkloads",
"wellarchitected:ListWorkloadShares",
"workdocs:CheckAlias",
"workdocs:Describe*",
"workdocs:Get*",
"workmail:Describe*",
"workmail:Get*",
"workmail:List*",
"workmail:Search*",
"workspaces-web:GetBrowserSettings",
"workspaces-web:GetIdentityProvider",
"workspaces-web:GetNetworkSettings",
"workspaces-web:GetPortal",
"workspaces-web:GetPortalServiceProviderMetadata",
"workspaces-web:GetTrustStore",
"workspaces-web:GetUserAccessLoggingSettings",
"workspaces-web:GetUserSettings",
"workspaces-web:ListBrowserSettings",
"workspaces-web:ListIdentityProviders",
"workspaces-web:ListNetworkSettings",
"workspaces-web:ListPortals",
"workspaces-web:ListTagsForResource",
"workspaces-web:ListTrustStores",
"workspaces-web:ListUserAccessLoggingSettings",
"workspaces-web:ListUserSettings",
"workspaces:Describe*",
"xray:BatchGet*",
"xray:Get*"
],
"Resource" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ResourceGroupsandTagEditorFullAccess

説明： Resource Groups とタグエディタへのフルアクセスを提供します。

ResourceGroupsandTagEditorFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ResourceGroupsandTagEditorFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

ポリシーのバージョン

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ResourceGroupsandTagEditorReadOnlyAccess

説明 : Resource Groups とタグエディタを使用するアクセスを許可しますが、タグエディタを介したタグの編集は許可しません。

ResourceGroupsandTagEditorReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ResourceGroupsandTagEditorReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:39 UTC
- 編集日時: 2023 年 8 月 10 日 13:42 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ResourceGroupsServiceRolePolicy

説明 : Resource Groups が AWS リソースを所有する AWS サービスをクエリしてグループを維持できるようにします up-to-date

ResourceGroupsServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2023 年 1 月 5 日 16:57 UTC
- 編集日時: 2023 年 1 月 5 日 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

説明: OpenShift Amazon EBS Container Storage Interface (CSI) ドライバーオペレーターが AWS、(ROSA) クラスターの Red Hat OpenShift Service に Amazon EBS CSI ドライバーをインストールして維持できるようにします。Amazon EBS CSI ドライバーは、ROSA クラスターが永続ボリューム用 Amazon EBS ボリュームのライフサイクルを管理できるようにします。

ROSAAmazonEBSCSIDriverOperatorPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAAmazonEBSCSIDriverOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 4 月 20 日 22:36 UTC
- 編集日時: 2023 年 4 月 20 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        ]
    }
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ROSACloudNetworkConfigOperatorPolicy

説明 : OpenShift Cloud Network Config Controller Operator が、AWS (ROSA) クラスターネットワークオーバーレイ上の Red Hat OpenShift Service で使用するネットワークリソースをプロビジョニングおよび管理できるようにします。OpenShift クラウドネットワークオペレーターは、を介してネットワークプラグインに代わって AWS APIs とインターフェイスします CustomResourceDefinitions。オペレーターはこれらのポリシー許可を使用し、ROSA クラスターの一部として Amazon EC2 インスタンスのプライベート IP アドレスを管理します。

ROSACloudNetworkConfigOperatorPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSACloudNetworkConfigOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:34 UTC
- 編集日時: 2023 年 4 月 20 日 22:34 UTC

- ARN: arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
        }
      }
    }
  ]
}
```



```
    }  
  }  
]  
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ROSAControlPlaneOperatorPolicy

説明 : Red Hat OpenShift Service on AWS (ROSA) コントロールプレーンが ROSA クラスターの Amazon EC2 および Amazon Route 53 リソースを管理できるようにします。

ROSAControlPlaneOperatorPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAControlPlaneOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 24 日 23:02 UTC
- 編集日時: 2023 年 6 月 30 日 21:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    ]
  }
}
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ROSAImageRegistryOperatorPolicy

説明 : OpenShift Image Registry Operator が、Red Hat OpenShift Service on AWS (ROSA) クラスター内イメージレジストリで使用する Amazon S3 バケットとオブジェクトをプロビジョニングおよび管理して、ROSA ストレージ要件を満たすことを許可します。 OpenShift Image Registry Operator は、Red Hat OpenShift クラスターの内部レジストリをインストールして維持します。

ROSAImageRegistryOperatorPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAImageRegistryOperatorPolicy をアタッチできません。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 4 月 27 日 20:13 UTC
- 編集日時: 2023 年 12 月 12 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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}/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSAIngressOperatorPolicy

説明 : OpenShift Ingress Operator が (ROSA) クラスターの Red Hat OpenShift Service のロードバランサーとドメインネームシステム AWS (DNS) 設定をプロビジョニングおよび管理できるようにします。このポリシーでは、タグ値への読み取りアクセスを許可します。オペレーターは Route 53 リソースのためにこのタグ値にフィルター処理を行い、ホストゾーンを検出します。

ROSAIngressOperatorPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAIngressOperatorPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:37 UTC
- 編集日時: 2023 年 4 月 20 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ROSAInstallerPolicy

説明： Red Hat OpenShift Service on AWS (ROSA) インストーラが ROSA クラスターのインストールをサポートする AWS リソースを管理できるようにします。これには ROSA ワーカーノードのインスタンスプロファイルの管理が含まれます。

ROSAInstallerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAInstallerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 6 日 21:00 UTC
- 編集日時: 2024 年 4 月 24 日 19:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ],
}
```

```
{
  "Sid" : "PassRoleToEC2",
  "Effect" : "Allow",
  "Action" : [
    "iam:PassRole"
  ],
  "Resource" : [
    "arn:*:iam:*:role/*-ROSA-Worker-Role"
  ],
  "Condition" : {
    "StringEquals" : {
      "iam:PassedToService" : [
        "ec2.amazonaws.com"
      ]
    }
  }
},
{
  "Sid" : "ManageInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteInstanceProfile",
    "iam:GetInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ]
},
{
  "Sid" : "CreateInstanceProfiles",
  "Effect" : "Allow",
  "Action" : [
    "iam>CreateInstanceProfile",
    "iam:TagInstanceProfile"
  ],
  "Resource" : [
    "arn:aws:iam:*:instance-profile/rosa-service-managed-*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "GetSecretValue",
    "Effect" : "Allow",
    "Action" : [
      "secretsmanager:GetSecretValue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "Route53ManageRecords",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeResourceRecordSets"
    ],
    "Resource" : "*",
    "Condition" : {
      "ForAllValues:StringLike" : {
        "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
          "*.openshiftapps.com",
          "*.devshift.org",
          "*.hypershift.local",
          "*.openshiftusgov.com",
          "*.devshiftusgov.com"
        ]
      }
    }
  },
  {
    "Sid" : "Route53Manage",
    "Effect" : "Allow",
    "Action" : [
      "route53:ChangeTagsForResource",
      "route53:CreateHostedZone",
      "route53>DeleteHostedZone"
    ],
  },
```

```
    "Resource" : "*"
  },
  {
    "Sid" : "CreateTags",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateTags"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : [
          "RunInstances"
        ]
      }
    }
  },
  {
    "Sid" : "RunInstancesNoCondition",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:snapshot*"
    ]
  },
  {
    "Sid" : "RunInstancesRestrictedRequestTag",
    "Effect" : "Allow",
    "Action" : "ec2:RunInstances",
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:volume*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  }
}
```

```
  },
  {
    "Sid" : "RunInstancesRedHatOwnedAMIs",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "ec2:Owner" : [
          "531415883065",
          "251351625822",
          "210686502322"
        ]
      }
    }
  },
  {
    "Sid" : "ManageInstancesRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
      "ec2:TerminateInstances",
      "ec2:GetConsoleOutput"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  },
  {
    "Sid" : "CreateGrantRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat" : "true"
      }
    }
  }
]
```

```
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    },
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    }
  }
},
{
  "Sid" : "ManagedKMSRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroups",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DeleteSecurityGroup",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DeleteSecurityGroup"
  ],
```



```
"Resource" : [
  "arn:aws:ec2:*:*:security-group*/*"
],
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/red-hat-managed" : "true"
  }
}
},
{
  "Sid" : "SecurityGroupIngressEgress",
  "Effect" : "Allow",
  "Action" : [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupEgress"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:security-group*/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateSecurityGroupsVPCNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateSecurityGroup"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "CreateTagsRestrictedActions",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
```

```
    "arn:aws:ec2:*:*:security-group/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:CreateAction" : [
        "CreateSecurityGroup"
      ]
    }
  }
},
{
  "Sid" : "CreateTagsK8sSubnet",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:subnet/*"
  ],
  "Condition" : {
    "ForAllValues:StringLike" : {
      "aws:TagKeys" : [
        "kubernetes.io/cluster/*"
      ]
    }
  }
},
{
  "Sid" : "ListPoliciesAttachedToRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAttachedRolePolicies",
    "iam:ListRolePolicies"
  ],
  "Resource" : "arn:aws:iam:*:*:role/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSAKMSProviderPolicy

説明: 組み込みの ROSA AWS 暗号化プロバイダーが Key Management Service (KMS) AWS キーを管理して、お客様が用意した AWS KMS キーを使用した etcd データ暗号化をサポートできるようにします。このポリシーでは、KMS キーを使用してデータの暗号化および復号化ができます。

ROSAKMSProviderPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAKMSProviderPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:10 UTC
- 編集日時: 2023 年 4 月 27 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "VolumeEncryption",
    "Effect" : "Allow",
    "Action" : [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat" : "true"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSAKubeControllerPolicy

説明： ROSA Kubernetes コントローラーが ROSA クラスターの Amazon EC2、Elastic Load Balancing (ELB)、および AWS Key Management Service (KMS) リソースを管理できるようにします。

ROSAKubeControllerPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAKubeControllerPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 27 日 20:09 UTC
- 編集日時: 2023 年 10 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSAManageSubscription

説明：このポリシーは、Red Hat OpenShift Service on AWS (ROSA) サブスクリプションを管理するために必要なアクセス許可を提供します。

ROSAManageSubscription は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAManageSubscription をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2022 年 4 月 11 日 20:58 UTC
- 編集日時: 2023 年 8 月 4 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSANodePoolManagementPolicy

説明 : Red Hat OpenShift Service on AWS (ROSA) が、セキュリティグループの設定やインスタンスとボリュームへのタグ付けなどのアクセス許可を含め、クラスター EC2 インスタンスをワーカーノードとして管理できるようにします。このポリシーでは、Key Management Service (KMS) AWS キーによって提供されるディスク暗号化で EC2 インスタンスを使用することもできます。

ROSANodePoolManagementPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSANodePoolManagementPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2023 年 6 月 8 日 20:48 UTC
- 編集日時: 2024 年 5 月 2 日 14:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ]
    }
  ]
}
```

```
    ],
    "Resource" : [
      "arn:*:iam:*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "PassWorkerRole",
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "arn:*:iam:*:role/*-ROSA-Worker-Role"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
    "Effect" : "Allow",
    "Action" : [
      "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:security-group-rule/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  }
},
```

```
{
  "Sid" : "NetworkInterfaces",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "NetworkInterfacesNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:ModifyNetworkInterfaceAttribute"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:vpc/*"
  ]
},
{
  "Sid" : "TerminateInstances",
  "Effect" : "Allow",
  "Action" : [
    "ec2:TerminateInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateTags",
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:CreateTags"
],
"Resource" : [
  "arn:aws:ec2:*:*:instance/*",
  "arn:aws:ec2:*:*:volume/*"
],
"Condition" : {
  "StringEquals" : {
    "ec2:CreateAction" : [
      "RunInstances"
    ]
  }
}
},
{
  "Sid" : "CreateTagsCAPAControllerReconcileInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "CreateTagsCAPAControllerReconcileVolume",
  "Effect" : "Allow",
  "Action" : [
    "ec2:CreateTags"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:volume/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "aws:RequestTag/red-hat-managed" : "true"
    }
  }
}
```

```
    }
  },
  {
    "Sid" : "RunInstancesRequest",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RunInstances"
    ],
    "Resource" : [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition" : {
      "StringEquals" : {
        "aws:RequestTag/red-hat-managed" : "true"
      }
    }
  }
},
{
  "Sid" : "RunInstancesNoCondition",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid" : "RunInstancesRedHatAMI",
  "Effect" : "Allow",
  "Action" : [
    "ec2:RunInstances"
  ],
  "Resource" : [
    "arn:aws:ec2:*:*:image/*"
  ],
  "Condition" : {
    "StringEquals" : {
      "ec2:Owner" : [
        "531415883065",
        "251351625822"
      ]
    }
  }
}
```



```
    ]
  }
}
},
{
  "Sid" : "ManagedKMSRestrictedResourceTag",
  "Effect" : "Allow",
  "Action" : [
    "kms:DescribeKey",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringLike" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
},
{
  "Sid" : "CreateGrantRestricted",
  "Effect" : "Allow",
  "Action" : [
    "kms:CreateGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : true
    },
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    },
    "StringLike" : {
      "kms:ViaService" : "ec2.*.amazonaws.com"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ROSASRESupportPolicy

説明: ROSA サイト信頼性エンジニアリング (SRE) に、ROSA クラスターノードの状態を変更する機能など、AWS (ROSA) クラスター上の Red Hat OpenShift Service に関連する AWS リソースを最初に監視、診断、サポートするために必要なアクセス許可を提供します。

ROSASRESupportPolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSASRESupportPolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 6 月 1 日 14:36 UTC
- 編集日時: 2024 年 4 月 10 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
```

```
"Effect" : "Allow",
"Action" : [
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeRegions",
  "sts:DecodeAuthorizationMessage"
],
"Resource" : "*"
},
{
  "Sid" : "Route53",
  "Effect" : "Allow",
  "Action" : [
    "route53:GetHostedZone",
    "route53:GetHostedZoneCount",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListResourceRecordSets"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeIAMRoles",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetRole",
    "iam:ListRoles"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "EC2DescribeInstance",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DescribeReservedInstances",
    "ec2:DescribeScheduledInstances"
  ],
  "Resource" : [
```

```
        "*"
    ]
},
{
    "Sid" : "VPCNetwork",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "Cloudtrail",
    "Effect" : "Allow",
    "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "Cloudwatch",
    "Effect" : "Allow",
    "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
    ],
    "Resource" : [
        "*"
    ]
},
{
    "Sid" : "DescribeVolumes",
    "Effect" : "Allow",
    "Action" : [
        "ec2:DescribeVolumes",
```

```
    "ec2:DescribeVolumesModifications",
    "ec2:DescribeVolumeStatus"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeLoadBalancers",
  "Effect" : "Allow",
  "Action" : [
    "elasticloadbalancing:DescribeAccountLimits",
    "elasticloadbalancing:DescribeInstanceHealth",
    "elasticloadbalancing:DescribeListenerCertificates",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeSSLPolicies",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeVPC",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcEndpointConnections",
    "ec2:DescribeVpcEndpoints"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Sid" : "DescribeSecurityGroups",
  "Effect" : "Allow",
```

```
"Action" : [
  "ec2:DescribeSecurityGroupReferences",
  "ec2:DescribeSecurityGroupRules",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeStaleSecurityGroups"
],
"Resource" : "*"
},
{
  "Sid" : "DescribeAddressesAttribute",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeAddressesAttribute",
  "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
},
{
  "Sid" : "DescribeInstance",
  "Effect" : "Allow",
  "Action" : [
    "iam:GetInstanceProfile"
  ],
  "Resource" : "arn:aws:iam:*:*:instance-profile/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DescribeSpotFleetInstances",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeSpotFleetInstances",
  "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
  "Condition" : {
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  }
},
{
  "Sid" : "DescribeVolumeAttribute",
  "Effect" : "Allow",
  "Action" : "ec2:DescribeVolumeAttribute",
  "Resource" : "arn:aws:ec2:*:*:volume/*",
  "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/red-hat-managed" : "true"
    }
  },
  {
    "Sid" : "ManageInstanceLifecycle",
    "Effect" : "Allow",
    "Action" : [
      "ec2:RebootInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource" : "arn:aws:ec2:*:*:instance/*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/red-hat-managed" : "true"
      }
    }
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ROSAWorkerInstancePolicy

説明: アカウントの AWS (ROSA) ワーカーノードで Red Hat OpenShift Service に Amazon EC2 インスタンスへの読み取り専用アクセスとコンピューティングノードのライフサイクル管理 AWS リージョン を許可します。

ROSAWorkerInstancePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ROSAWorkerInstancePolicy をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2023 年 4 月 20 日 22:35 UTC
- 編集日時: 2023 年 4 月 20 日 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

Route53RecoveryReadinessServiceRolePolicy

説明: Route 53 Recovery Readiness のサービスリンクロールポリシー

Route53RecoveryReadinessServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2021 年 7 月 15 日 16:06 UTC
- 編集日時: 2023 年 2 月 14 日 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

Route53ResolverServiceRolePolicy

説明： Route53 Resolver が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします

Route53ResolverServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 8 月 12 日 17:47 UTC
- 編集日時: 2020 年 8 月 12 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

S3StorageLensServiceRolePolicy

説明 : S3 Storage Lens が使用または管理する AWS のサービス およびリソースへのアクセスを有効にする

S3StorageLensServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2020 年 11 月 18 日 18:15 UTC
- 編集日時: 2020 年 11 月 18 日 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

SecretsManagerReadWrite

説明： 経由で AWS Secrets Manager への読み取り/書き込みアクセスを提供します AWS Management Console。注：これは IAM アクションを除外するため、ローテーション設定 FullAccess が必要な場合は IAM と組み合わせてください。

SecretsManagerReadWrite は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに SecretsManagerReadWrite をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 4 月 4 日 18:05 UTC
- 編集日時: 2024 年 2 月 22 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

ポリシーのバージョン

ポリシーのバージョン: v5 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
    ]
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

SecurityAudit

説明：セキュリティ監査テンプレートは、セキュリティ設定メタデータを読み取るためのアクセス権を付与します。AWS アカウントの設定を監査するソフトウェアに便利です。

SecurityAudit は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに SecurityAudit をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2024 年 4 月 5 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/SecurityAudit

ポリシーのバージョン

ポリシーのバージョン: v42 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
```

```
"acm-pca:DescribeCertificateAuthority",
"acm-pca:DescribeCertificateAuthorityAuditReport",
"acm-pca:GetPolicy",
"acm-pca:ListCertificateAuthorities",
"acm-pca:ListPermissions",
"acm-pca:ListTags",
"acm:Describe*",
"acm:List*",
"airflow:GetEnvironment",
"airflow:ListEnvironments",
"appflow:ListFlows",
"appflow:ListTagsForResource",
"application-autoscaling:Describe*",
"appmesh:Describe*",
"appmesh:List*",
"apprunner:DescribeAutoScalingConfiguration",
"apprunner:DescribeCustomDomains",
"apprunner:DescribeObservabilityConfiguration",
"apprunner:DescribeService",
"apprunner:DescribeVpcConnector",
"apprunner:DescribeVpcIngressConnection",
"apprunner:ListAutoScalingConfigurations",
"apprunner:ListConnections",
"apprunner:ListObservabilityConfigurations",
"apprunner:ListOperations",
"apprunner:ListServices",
"apprunner:ListTagsForResource",
"apprunner:ListVpcConnectors",
"apprunner:ListVpcIngressConnections",
"appsync:GetApiCache",
"appsync:List*",
"athena:GetWorkGroup",
"athena:List*",
"auditmanager:GetAccountStatus",
"auditmanager:ListAssessmentControlInsightsByControlDomain",
"auditmanager:ListAssessmentFrameworkShareRequests",
"auditmanager:ListAssessmentFrameworks",
"auditmanager:ListAssessmentReports",
"auditmanager:ListAssessments",
"auditmanager:ListControlDomainInsights",
"auditmanager:ListControlDomainInsightsByAssessment",
"auditmanager:ListControlInsightsByControlDomain",
"auditmanager:ListControls",
"auditmanager:ListNotifications",
```

```
"auditmanager:ListTagsForResource",
"autoscaling-plans:DescribeScalingPlans",
"autoscaling:Describe*",
"backup:DescribeGlobalSettings",
"backup:DescribeRegionSettings",
"backup:GetBackupVaultAccessPolicy",
"backup:GetBackupVaultNotifications",
"backup:ListBackupVaults",
"backup:ListTags",
"batch:DescribeComputeEnvironments",
"batch:DescribeJobDefinitions",
"bedrock:GetCustomModel",
"bedrock:GetModelInvocationLoggingConfiguration",
"bedrock:ListCustomModels",
"bedrock:ListTagsForResource",
"braket:SearchJobs",
"braket:SearchQuantumTasks",
"chime:List*",
"cloud9:Describe*",
"cloud9:ListEnvironments",
"clouddirectory:ListDirectories",
"cloudformation:DescribeStack*",
"cloudformation:GetStackPolicy",
"cloudformation:GetTemplate",
"cloudformation:ListStack*",
"cloudfront:Get*",
"cloudfront:List*",
"cloudsearch:DescribeDomainEndpointOptions",
"cloudsearch:DescribeDomains",
"cloudsearch:DescribeServiceAccessPolicies",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetInsightSelectors",
"cloudtrail:GetTrail",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudtrail:ListTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Describe*",
"cloudwatch:GetDashboard",
"cloudwatch:ListDashboards",
"cloudwatch:ListTagsForResource",
"codeartifact:GetDomainPermissionsPolicy",
"codeartifact:GetRepositoryPermissionsPolicy",
```

```
"codeartifact:ListRepositories",
"codebuild:BatchGetProjects",
"codebuild:GetResourcePolicy",
"codebuild:ListProjects",
"codecommit:BatchGetRepositories",
"codecommit:GetBranch",
"codecommit:GetObjectIdentifier",
"codecommit:GetRepository",
"codecommit:GetRepositoryTriggers",
"codecommit:List*",
"codedeploy:Batch*",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:GetJobDetails",
"codepipeline:GetPipeline",
"codepipeline:GetPipelineExecution",
"codepipeline:GetPipelineState",
"codepipeline:ListPipelines",
"codestar:Describe*",
"codestar:List*",
"cognito-identity:Describe*",
"cognito-identity:GetIdentityPoolRoles",
"cognito-identity:ListIdentityPools",
"cognito-identity:ListTagsForResource",
"cognito-idp:Describe*",
"cognito-idp:ListDevices",
"cognito-idp:ListGroups",
"cognito-idp:ListIdentityProviders",
"cognito-idp:ListResourceServers",
"cognito-idp:ListTagsForResource",
"cognito-idp:ListUserImportJobs",
"cognito-idp:ListUserPoolClients",
"cognito-idp:ListUserPools",
"cognito-idp:ListUsers",
"cognito-idp:ListUsersInGroup",
"cognito-sync:Describe*",
"cognito-sync:List*",
"comprehend:Describe*",
"comprehend:List*",
"comprehendmedical:ListICD10CMInferenceJobs",
"comprehendmedical:ListPHIDetectionJobs",
"comprehendmedical:ListRxNormInferenceJobs",
"comprehendmedical:ListSNOMEDCTInferenceJobs",
"config:BatchGetAggregateResourceConfig",
```

```
"config:BatchGetResourceConfig",
"config:Deliver*",
"config:Describe*",
"config:Get*",
"config:List*",
"config>SelectAggregateResourceConfig",
"config>SelectResourceConfig",
"connect:ListApprovedOrigins",
"connect:ListInstanceAttributes",
"connect:ListInstanceStorageConfigs",
"connect:ListInstances",
"connect:ListIntegrationAssociations",
"connect:ListLambdaFunctions",
"connect:ListLexBots",
"connect:ListSecurityKeys",
"databrew:DescribeDataset",
"databrew:DescribeProject",
"databrew:ListJobs",
"databrew:ListProjects",
"dataexchange:ListDataSets",
"datapipeline:DescribeObjects",
"datapipeline:DescribePipelines",
"datapipeline:EvaluateExpression",
"datapipeline:GetPipelineDefinition",
"datapipeline:ListPipelines",
"datapipeline:QueryObjects",
"datapipeline:ValidatePipelineDefinition",
"datasync:Describe*",
"datasync:List*",
"dax:Describe*",
"dax:ListTags",
"deepracer:ListModels",
"detective:GetGraphIngestState",
"detective:ListGraphs",
"detective:ListMembers",
"devicefarm:ListProjects",
"directconnect:Describe*",
"discovery:DescribeAgents",
"discovery:DescribeConfigurations",
"discovery:DescribeContinuousExports",
"discovery:DescribeExportConfigurations",
"discovery:DescribeExportTasks",
"discovery:DescribeImportTasks",
"dms:Describe*",
```

```
"dms:ListTagsForResource",
"docdb-elastic:ListClusters",
"ds:DescribeDirectories",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeExport",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeKinesisStreamingDestination",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListExports",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:Describe*",
"ec2:GetEbsEncryptionByDefault",
"ec2:GetImageBlockPublicAccessState",
"ec2:GetManagedPrefixListAssociations",
"ec2:GetManagedPrefixListEntries",
"ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
"ec2:GetNetworkInsightsAccessScopeContent",
"ec2:GetTransitGatewayAttachmentPropagations",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:SearchTransitGatewayRoutes",
"ecr-public:DescribeImageTags",
"ecr-public:DescribeImages",
"ecr-public:DescribeRegistries",
"ecr-public:DescribeRepositories",
"ecr-public:GetRegistryCatalogData",
"ecr-public:GetRepositoryCatalogData",
"ecr-public:GetRepositoryPolicy",
"ecr-public:ListTagsForResource",
"ecr:BatchGetRepositoryScanningConfiguration",
"ecr:DescribeImageScanFindings",
"ecr:DescribeImages",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:GetLifecyclePolicy",
"ecr:GetRegistryPolicy",
"ecr:GetRegistryScanningConfiguration",
```



```
"ecr:GetRepositoryPolicy",
"ecr:ListImages",
"ecr:ListTagsForResource",
"ecs:Describe*",
"ecs:List*",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodeGroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodeGroups",
"eks:ListTagsForResource",
"eks:ListUpdates",
"elastic-inference:DescribeAccelerators",
"elasticache:Describe*",
"elasticache:ListTagsForResource",
"elasticbeanstalk:Describe*",
"elasticbeanstalk:ListTagsForResource",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeAccountPreferences",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeReplicationConfigurations",
"elasticfilesystem:DescribeTags",
"elasticloadbalancing:Describe*",
"elasticmapreduce:Describe*",
"elasticmapreduce:GetAutoTerminationPolicy",
"elasticmapreduce:GetBlockPublicAccessConfiguration",
"elasticmapreduce:GetManagedScalingPolicy",
"elasticmapreduce:ListClusters",
"elasticmapreduce:ListInstances",
"elasticmapreduce:ListSecurityConfigurations",
"elastictranscoder:ListPipelines",
"emr-serverless:GetApplication",
"emr-serverless:ListApplications",
"emr-serverless:ListJobRuns",
"es:Describe*",
"es:GetCompatibleVersions",
"es:ListDomainNames",
"es:ListElasticsearchInstanceTypeDetails",
```

```
"es:ListElasticsearchVersions",
"es:ListTags",
"events:Describe*",
"events:List*",
"events:TestEventPattern",
"finspace:ListEnvironments",
"finspace:ListKxEnvironments",
"firehose:Describe*",
"firehose:List*",
"fms:ListComplianceStatus",
"fms:ListPolicies",
"forecast:ListDatasets",
"frauddetector:GetDetectors",
"fsx:Describe*",
"fsx:List*",
"gamelift:ListBuilds",
"gamelift:ListFleets",
"geo:ListMaps",
"glacier:DescribeVault",
"glacier:GetDataRetrievalPolicy",
"glacier:GetVaultAccessPolicy",
"glacier:GetVaultLock",
"glacier:ListVaults",
"globalaccelerator:Describe*",
"globalaccelerator:List*",
"glue:GetCrawlers",
"glue:GetDataCatalogEncryptionSettings",
"glue:GetDatabases",
"glue:GetDevEndpoints",
"glue:GetJobs",
"glue:GetResourcePolicy",
"glue:GetSecurityConfiguration",
"glue:GetSecurityConfigurations",
"glue:GetTags",
"grafana:ListWorkspaces",
"greengrass:List*",
"guardduty:DescribePublishingDestination",
"guardduty:Get*",
"guardduty:List*",
"health:DescribeAffectedAccountsForOrganization",
"health:DescribeAffectedEntities",
"health:DescribeAffectedEntitiesForOrganization",
"health:DescribeEntityAggregates",
"health:DescribeEventAggregates",
```

```
"health:DescribeEventDetails",
"health:DescribeEventDetailsForOrganization",
"health:DescribeEventTypes",
"health:DescribeEvents",
"health:DescribeEventsForOrganization",
"health:DescribeHealthServiceStatusForOrganization",
"healthlake:ListFHIRDatastores",
"honeycode:ListTables",
"iam:GenerateCredentialReport",
"iam:GenerateServiceLastAccessedDetails",
"iam:Get*",
"iam:List*",
"iam:SimulateCustomPolicy",
"iam:SimulatePrincipalPolicy",
"identitystore:ListGroupMemberships",
"identitystore:ListGroupMembershipsForMember",
"identitystore:ListGroups",
"identitystore:ListUsers",
"inspector2:BatchGetAccountStatus",
"inspector2:BatchGetFreeTrialInfo",
"inspector2:DescribeOrganizationConfiguration",
"inspector2:GetConfiguration",
"inspector2:GetDelegatedAdminAccount",
"inspector2:GetFindingsReportStatus",
"inspector2:GetMember",
"inspector2:ListAccountPermissions",
"inspector2:ListCoverage",
"inspector2:ListCoverageStatistics",
"inspector2:ListDelegatedAdminAccounts",
"inspector2:ListFilters",
"inspector2:ListFindingAggregations",
"inspector2:ListFindings",
"inspector2:ListTagsForResource",
"inspector2:ListUsageTotals",
"inspector:Describe*",
"inspector:Get*",
"inspector:List*",
"inspector:Preview*",
"iot:Describe*",
"iot:GetPolicy",
"iot:GetPolicyVersion",
"iot:List*",
"iotanalytics:ListChannels",
"iotevents:ListInputs",
```

```
"iotfleetwise:ListModelManifests",
"iotsitewise:DescribeGatewayCapabilityConfiguration",
"iotsitewise:ListAssetModels",
"iotsitewise:ListGateways",
"iottwinmaker:ListWorkspaces",
"kafka-cluster:Describe*",
"kafka:Describe*",
"kafka:GetBootstrapBrokers",
"kafka:GetCompatibleKafkaVersions",
"kafka:List*",
"kafkaconnect:Describe*",
"kafkaconnect:List*",
"kendra:DescribeIndex",
"kendra:ListDataSources",
"kendra:ListIndices",
"kendra:ListTagsForResource",
"kinesis:DescribeLimits",
"kinesis:DescribeStream",
"kinesis:DescribeStreamConsumer",
"kinesis:DescribeStreamSummary",
"kinesis:ListShards",
"kinesis:ListStreamConsumers",
"kinesis:ListStreams",
"kinesis:ListTagsForStream",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kinesisvideo:DescribeEdgeConfiguration",
"kinesisvideo:DescribeMappedResourceConfiguration",
"kinesisvideo:DescribeMediaStorageConfiguration",
"kinesisvideo:DescribeNotificationConfiguration",
"kinesisvideo:DescribeSignalingChannel",
"kinesisvideo:DescribeStream",
"kinesisvideo:ListSignalingChannels",
"kinesisvideo:ListStreams",
"kinesisvideo:ListTagsForResource",
"kinesisvideo:ListTagsForStream",
"kms:Describe*",
"kms:Get*",
"kms:List*",
"lambda:GetAccountSettings",
"lambda:GetFunctionConfiguration",
"lambda:GetFunctionEventInvokeConfig",
"lambda:GetLayerVersionPolicy",
"lambda:GetPolicy",
```

```
"lambda:List*",
"lex:DescribeBot",
"lex:DescribeResourcePolicy",
"lex:ListBots",
"license-manager:List*",
"lightsail:GetBuckets",
"lightsail:GetContainerServices",
"lightsail:GetDiskSnapshots",
"lightsail:GetDisks",
"lightsail:GetInstances",
"lightsail:GetLoadBalancers",
"logs:Describe*",
"logs:ListTagsForResource",
"logs:ListTagsLogGroup",
"lookoutequipment:ListDatasets",
"lookoutmetrics:ListAnomalyDetectors",
"lookoutvision:ListProjects",
"machinelearning:DescribeMLModels",
"macie2:ListFindings",
"managedblockchain:ListNetworks",
"mechanicalturk:ListHITs",
"mediaconnect:Describe*",
"mediaconnect:List*",
"medialive:ListChannels",
"mediapackage-vod:DescribePackagingGroup",
"mediapackage-vod:ListPackagingGroups",
"mediapackage:DescribeOriginEndpoint",
"mediapackage:ListOriginEndpoints",
"mediastore:GetContainerPolicy",
"mediastore:GetCorsPolicy",
"mediastore:ListContainers",
"memorydb:DescribeClusters",
"mq:DescribeBroker",
"mq:DescribeBrokerEngineTypes",
"mq:DescribeBrokerInstanceOptions",
"mq:DescribeConfiguration",
"mq:DescribeConfigurationRevision",
"mq:DescribeUser",
"mq:ListBrokers",
"mq:ListConfigurationRevisions",
"mq:ListConfigurations",
"mq:ListTags",
"mq:ListUsers",
"network-firewall:DescribeFirewall",
```

```
"network-firewall:DescribeFirewallPolicy",
"network-firewall:DescribeLoggingConfiguration",
"network-firewall:DescribeResourcePolicy",
"network-firewall:DescribeRuleGroup",
"network-firewall:ListFirewallPolicies",
"network-firewall:ListFirewalls",
"network-firewall:ListRuleGroups",
"networkmanager:DescribeGlobalNetworks",
"nimble:ListStudios",
"opsworks-cm:DescribeServers",
"opsworks:DescribeStacks",
"organizations:Describe*",
"organizations:List*",
"personalize:DescribeDatasetGroup",
"personalize:ListDatasetGroups",
"private-networks:ListNetworks",
"profile:GetDomain",
"profile:ListDomains",
"profile:ListIntegrations",
"qldb:DescribeJournalS3Export",
"qldb:DescribeLedger",
"qldb:ListJournalS3Exports",
"qldb:ListJournalS3ExportsForLedger",
"qldb:ListLedgers",
"quicksight:Describe*",
"quicksight:List*",
"ram:GetResourceShares",
"ram:List*",
"rds:Describe*",
"rds:DownloadDBLogFilePortion",
"rds:ListTagsForResource",
"redshift-serverless:GetNamespace",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:Describe*",
"rekognition:Describe*",
"rekognition:List*",
"resource-groups:ListGroupResources",
"robomaker:Describe*",
"robomaker:List*",
"route53:Get*",
"route53:List*",
"route53domains:GetDomainDetail",
"route53domains:GetOperationDetail",
```

```
"route53domains:ListDomains",
"route53domains:ListOperations",
"route53domains:ListTagsForDomain",
"route53resolver:Get*",
"route53resolver:List*",
"s3-outposts:ListEndpoints",
"s3-outposts:ListOutpostsWithS3",
"s3-outposts:ListSharedEndpoints",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetMultiRegionAccessPointPolicy",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"s3:ListMultiRegionAccessPoints",
"sagemaker:Describe*",
"sagemaker:List*",
"schemas:DescribeCodeBinding",
"schemas:DescribeDiscoverer",
"schemas:DescribeRegistry",
"schemas:DescribeSchema",
"schemas:GetResourcePolicy",
"schemas:ListDiscoverers",
"schemas:ListRegistries",
"schemas:ListSchemaVersions",
"schemas:ListSchemas",
"schemas:ListTagsForResource",
"sdb:DomainMetadata",
"sdb:ListDomains",
"secretsmanager:DescribeSecret",
"secretsmanager:GetResourcePolicy",
"secretsmanager:ListSecretVersionIds",
"secretsmanager:ListSecrets",
```

```
"securityhub:Describe*",
"securityhub:Get*",
"securityhub:List*",
"serverlessrepo:GetApplicationPolicy",
"serverlessrepo:List*",
"servicequotas:GetAWSDefaultServiceQuota",
"servicequotas:GetAssociationForServiceQuotaTemplate",
"servicequotas:GetRequestedServiceQuotaChange",
"servicequotas:GetServiceQuota",
"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
"servicequotas:ListAWSDefaultServiceQuotas",
"servicequotas:ListRequestedServiceQuotaChangeHistory",
"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
"servicequotas:ListServiceQuotas",
"servicequotas:ListServices",
"servicequotas:ListTagsForResource",
"ses:Describe*",
"ses:GetAccount",
"ses:GetAccountSendingEnabled",
"ses:GetConfigurationSet",
"ses:GetConfigurationSetEventDestinations",
"ses:GetDedicatedIps",
"ses:GetEmailIdentity",
"ses:GetIdentityDkimAttributes",
"ses:GetIdentityPolicies",
"ses:GetIdentityVerificationAttributes",
"ses:ListConfigurationSets",
"ses:ListDedicatedIpPools",
"ses:ListIdentities",
"ses:ListIdentityPolicies",
"ses:ListReceiptFilters",
"ses:ListReceiptRuleSets",
"ses:ListVerifiedEmailAddresses",
"shield:Describe*",
"shield:GetSubscriptionState",
"shield:List*",
"snowball:ListClusters",
"snowball:ListJobs",
"sns:GetPlatformApplicationAttributes",
"sns:GetTopicAttributes",
"sns:ListSubscriptions",
"sns:ListSubscriptionsByTopic",
"sns:ListTagsForResource",
```



```
"sns:ListTopics",
"sqs:GetQueueAttributes",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListQueueTags",
"sqs:ListQueues",
"ssm:Describe*",
"ssm:GetAutomationExecution",
"ssm:GetServiceSetting",
"ssm:ListAssociationVersions",
"ssm:ListAssociations",
"ssm:ListCommands",
"ssm:ListComplianceItems",
"ssm:ListComplianceSummaries",
"ssm:ListDocumentMetadataHistory",
"ssm:ListDocumentVersions",
"ssm:ListDocuments",
"ssm:ListInventoryEntries",
"ssm:ListOpsMetadata",
"ssm:ListResourceComplianceSummaries",
"ssm:ListResourceDataSync",
"ssm:ListTagsForResource",
"sso:DescribeAccountAssignmentCreationStatus",
"sso:DescribePermissionSet",
"sso:DescribePermissionsPolicies",
"sso:List*",
"states:DescribeStateMachine",
"states:ListStateMachines",
"storagegateway:DescribeBandwidthRateLimit",
"storagegateway:DescribeCache",
"storagegateway:DescribeCachediSCSIVolumes",
"storagegateway:DescribeGatewayInformation",
"storagegateway:DescribeMaintenanceStartTime",
"storagegateway:DescribeNFSFileShares",
"storagegateway:DescribeSnapshotSchedule",
"storagegateway:DescribeStorediSCSIVolumes",
"storagegateway:DescribeTapeArchives",
"storagegateway:DescribeTapeRecoveryPoints",
"storagegateway:DescribeTapes",
"storagegateway:DescribeUploadBuffer",
"storagegateway:DescribeVTLDevices",
"storagegateway:DescribeWorkingStorage",
"storagegateway:List*",
"sts:GetAccessKeyInfo",
"support:DescribeTrustedAdvisorCheckRefreshStatuses",
```

```
"support:DescribeTrustedAdvisorCheckResult",
"support:DescribeTrustedAdvisorCheckSummaries",
"support:DescribeTrustedAdvisorChecks",
"synthetics:DescribeCanaries",
"synthetics:DescribeCanariesLastRun",
"synthetics:DescribeRuntimeVersions",
"synthetics:GetCanary",
"synthetics:GetCanaryRuns",
"synthetics:GetGroup",
"synthetics>ListAssociatedGroups",
"synthetics>ListGroupResources",
"synthetics>ListGroups",
"synthetics>ListTagsForResource",
"tag:GetResources",
"tag:GetTagKeys",
"transcribe:GetCallAnalyticsCategory",
"transcribe:GetMedicalVocabulary",
"transcribe:GetVocabulary",
"transcribe:GetVocabularyFilter",
"transcribe>ListCallAnalyticsCategories",
"transcribe>ListCallAnalyticsJobs",
"transcribe>ListLanguageModels",
"transcribe>ListMedicalTranscriptionJobs",
"transcribe>ListMedicalVocabularies",
"transcribe>ListTagsForResource",
"transcribe>ListTranscriptionJobs",
"transcribe>ListVocabularies",
"transcribe>ListVocabularyFilters",
"transfer:Describe*",
"transfer>List*",
"translate>List*",
"trustedadvisor:Describe*",
"voiceid:DescribeDomain",
"waf-regional:GetWebACL",
"waf-regional>ListResourcesForWebACL",
"waf-regional>ListTagsForResource",
"waf-regional>ListWebACLs",
"waf:GetWebACL",
"waf>ListTagsForResource",
"waf>ListWebACLs",
"wafv2:GetLoggingConfiguration",
"wafv2:GetWebACL",
"wafv2:GetWebACLForResource",
"wafv2>ListAvailableManagedRuleGroups",
```

```
    "wafv2:ListIPSets",
    "wafv2:ListLoggingConfigurations",
    "wafv2:ListRegexPatternSets",
    "wafv2:ListResourcesForWebACL",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "wafv2:ListWebACLs",
    "wisdom:GetAssistant",
    "workdocs:DescribeResourcePermissions",
    "workspaces:Describe*",
    "xray:GetEncryptionConfig",
    "xray:GetGroup",
    "xray:GetGroups",
    "xray:GetSamplingRules",
    "xray:GetSamplingTargets",
    "xray:GetTraceSummaries",
    "xray:ListTagsForResource"
  ],
  "Resource" : "*"
},
{
  "Sid" : "APIGatewayAccess",
  "Effect" : "Allow",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis",
    "arn:aws:apigateway:*::/apis/*/authorizers/*",
    "arn:aws:apigateway:*::/apis/*/authorizers",
    "arn:aws:apigateway:*::/apis/*/cors",
    "arn:aws:apigateway:*::/apis/*/deployments/*",
    "arn:aws:apigateway:*::/apis/*/deployments",
    "arn:aws:apigateway:*::/apis/*/exports/*",
    "arn:aws:apigateway:*::/apis/*/integrations/*",
    "arn:aws:apigateway:*::/apis/*/integrations",
    "arn:aws:apigateway:*::/apis/*/models/*",
    "arn:aws:apigateway:*::/apis/*/models",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/apis/*/stages",
    "arn:aws:apigateway:*::/apis/*/stages/*",
    "arn:aws:apigateway:*::/clientcertificates",
    "arn:aws:apigateway:*::/clientcertificates/*",
```

```
"arn:aws:apigateway:*::/domainnames",
"arn:aws:apigateway:*::/domainnames/*/apimappings",
"arn:aws:apigateway:*::/restapis",
"arn:aws:apigateway:*::/restapis/*/authorizers/*",
"arn:aws:apigateway:*::/restapis/*/authorizers",
"arn:aws:apigateway:*::/restapis/*/deployments/*",
"arn:aws:apigateway:*::/restapis/*/deployments",
"arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
"arn:aws:apigateway:*::/restapis/*/documentation/parts",
"arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
"arn:aws:apigateway:*::/restapis/*/documentation/versions",
"arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
"arn:aws:apigateway:*::/restapis/*/gatewayresponses",
"arn:aws:apigateway:*::/restapis/*/models/*",
"arn:aws:apigateway:*::/restapis/*/models",
"arn:aws:apigateway:*::/restapis/*/requestvalidators",
"arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
"arn:aws:apigateway:*::/restapis/*/resources/*",
"arn:aws:apigateway:*::/restapis/*/resources",
"arn:aws:apigateway:*::/restapis/*/stages",
"arn:aws:apigateway:*::/restapis/*/stages/*",
"arn:aws:apigateway:*::/tags/*",
"arn:aws:apigateway:*::/vpclinks"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

SecurityLakeServiceLinkedRole

説明：このポリシーは、ユーザーに代わって Amazon Security Lake サービスを運用するアクセス許可を付与します。

SecurityLakeServiceLinkedRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2022 年 11 月 29 日 14:03 UTC
- 編集日時: 2024 年 4 月 19 日 16:00 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
}
```

```
{
  "Sid" : "DescribeOrgAccounts",
  "Effect" : "Allow",
  "Action" : [
    "organizations:DescribeAccount"
  ],
  "Resource" : [
    "arn:aws:organizations::*:account/o-*/*"
  ]
},
{
  "Sid" : "AllowManagementOfServiceLinkedChannel",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:CreateServiceLinkedChannel",
    "cloudtrail>DeleteServiceLinkedChannel",
    "cloudtrail:GetServiceLinkedChannel",
    "cloudtrail:UpdateServiceLinkedChannel"
  ],
  "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
},
{
  "Sid" : "AllowListServiceLinkedChannel",
  "Effect" : "Allow",
  "Action" : [
    "cloudtrail:ListServiceLinkedChannels"
  ],
  "Resource" : "*"
},
{
  "Sid" : "DescribeAnyVpc",
  "Effect" : "Allow",
  "Action" : [
    "ec2:DescribeVpcs"
  ],
  "Resource" : "*"
},
{
  "Sid" : "ListDelegatedAdmins",
  "Effect" : "Allow",
  "Action" : [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource" : "*",
```

```
    "Condition" : {
      "StringEquals" : {
        "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "AllowWafLoggingConfiguration",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:PutLoggingConfiguration",
      "wafv2:GetLoggingConfiguration",
      "wafv2:ListLoggingConfigurations",
      "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "wafv2:LogScope" : "SecurityLake"
      }
    }
  },
  {
    "Sid" : "AllowPutLoggingConfiguration",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:PutLoggingConfiguration"
    ],
    "Resource" : "*",
    "Condition" : {
      "ArnLike" : {
        "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
      }
    }
  },
  {
    "Sid" : "ListWebACLs",
    "Effect" : "Allow",
    "Action" : [
      "wafv2:ListWebACLs"
    ],
    "Resource" : "*"
  },
  {
```

```
"Sid" : "LogDelivery",
"Effect" : "Allow",
"Action" : [
  "logs:CreateLogDelivery",
  "logs>DeleteLogDelivery"
],
"Resource" : "*",
"Condition" : {
  "ForAnyValue:StringEquals" : {
    "aws:CalledVia" : [
      "wafv2.amazonaws.com"
    ]
  }
}
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ServerMigration_ServiceRole

説明: AWS Server Migration Service が VMs を EC2 に移行できるようにするアクセス許可: Server Migration Service が移行したリソースを顧客の EC2 アカウントに配置することを許可します。

ServerMigration_ServiceRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigration_ServiceRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2020 年 8 月 11 日 20:41 UTC
- 編集日時: 2020 年 10 月 15 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*/*"
    }
  }
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ServerMigrationConnector

説明： AWS Server Migration Connector が VMs を EC2 に移行できるようにするアクセス許可。AWS Server Migration Service との通信、「sms-b-」とimport-to-ec「2-」で始まる S3 バケットへの読み取り/書き込みアクセス、および AWS Server Migration Connector のアップグレード、での AWS Server Migration Connector 登録 AWS、へのメトリクスのアップロードに使用されるバケットを許可します AWS。

ServerMigrationConnector は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigrationConnector をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2016 年 10 月 24 日 21:45 UTC
- 編集日時: 2016 年 10 月 24 日 21:45 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationConnector

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ServerMigrationServiceConsoleFullAccess

説明： Server Migration Service Console のすべての機能を使用するために必要なアクセス許可

ServerMigrationServiceConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigrationServiceConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2020 年 5 月 9 日 17:18 UTC
- 編集日時: 2020 年 7 月 20 日 22:00 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ServerMigrationServiceLaunchRole

説明：移行された AWS サーバーとアプリケーション AWS アカウント を起動するために、サーバー移行サービスが関連する AWS リソースを作成してお客様の に更新できるようにするアクセス許可。

ServerMigrationServiceLaunchRole は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigrationServiceLaunchRole をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2018 年 11 月 26 日 19:53 UTC
- 編集日時: 2020 年 10 月 15 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、 はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

ServerMigrationServiceRoleForInstanceValidation

説明：AWS SMS が使用済みデータ検証スクリプトを実行し、スクリプトの成功/失敗を SMS に送信できるようにするアクセス許可

ServerMigrationServiceRoleForInstanceValidation は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServerMigrationServiceRoleForInstanceValidation をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー

- 作成日時: 2020 年 7 月 20 日 22:25 UTC
- 編集日時: 2020 年 7 月 20 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ServiceQuotasFullAccess

説明： Service Quotas へのフルアクセスを提供します

ServiceQuotasFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServiceQuotasFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 24 日 15:44 UTC
- 編集日時: 2021 年 2 月 4 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

ポリシーのバージョン

ポリシーのバージョン: v4 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
    }
  }
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ServiceQuotasReadOnlyAccess

説明： Service Quotas への読み取り専用アクセスを提供します

ServiceQuotasReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ServiceQuotasReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 6 月 24 日 15:31 UTC
- 編集日時: 2020 年 12 月 21 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ServiceQuotasServiceRolePolicy

説明： Service Quotas がユーザーに代わってサポートケースを作成することを許可する

ServiceQuotasServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 5 月 22 日 20:44 UTC
- 編集日時: 2019 年 6 月 24 日 14:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

SimpleWorkflowFullAccess

説明 : Simple Workflow 設定サービスへのフルアクセスを提供します。

SimpleWorkflowFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに SimpleWorkflowFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2015 年 2 月 6 日 18:41 UTC
- 編集日時: 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/SimpleWorkflowFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

SplitCostAllocationDataServiceRolePolicy

説明: 該当する場合は、分割コスト配分データで AWS Organizations 情報を取得し、顧客がオプトインした分割コスト配分データサービスのテレメトリデータを収集できるようにします。

SplitCostAllocationDataServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2024 年 4 月 16 日 16:05 UTC
- 編集日時: 2024 年 4 月 16 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
```

```
    "organizations:ListAccounts",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListParents"
  ],
  "Resource" : "*"
},
{
  "Sid" : "AmazonManagedServiceForPrometheusAccess",
  "Effect" : "Allow",
  "Action" : [
    "aps:ListWorkspaces",
    "aps:QueryMetrics"
  ],
  "Resource" : "*"
}
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

SupportUser

説明：このポリシーは、の問題をトラブルシューティングして解決するためのアクセス許可を付与します AWS アカウント。このポリシーにより、ユーザーは AWS サポートに連絡してケースを作成および管理することもできます。

SupportUser は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに SupportUser をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:21 UTC
- 編集日時: 2023 年 8 月 25 日 18:40 UTC

- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

ポリシーのバージョン

ポリシーのバージョン: v8 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

SystemAdministrator

説明: アプリケーションおよび開発オペレーションに必要なリソースに必要なフルアクセス許可を付与します。

SystemAdministrator は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに SystemAdministrator をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:23 UTC
- 編集日時: 2020 年 8 月 24 日 20:05 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

ポリシーのバージョニング

ポリシーのバージョン: v6 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

TranslateFullAccess

説明： Amazon Translate へのフルアクセスを提供します。

TranslateFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに TranslateFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 27 日 23:36 UTC
- 編集日時: 2020 年 1 月 8 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

TranslateReadOnly

説明： Amazon Translate への読み取り専用アクセスを提供します。

TranslateReadOnly は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに TranslateReadOnly をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2017 年 11 月 29 日 18:22 UTC
- 編集日時: 2023 年 5 月 24 日 17:19 UTC

- ARN: arn:aws:iam::aws:policy/TranslateReadOnly

ポリシーのバージョン

ポリシーのバージョン: v7 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)

- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

ViewOnlyAccess

説明: このポリシーは、すべての AWS サービスでリソースと基本メタデータを表示するアクセス許可を付与します。

ViewOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに ViewOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: ジョブ機能ポリシー
- 作成日時: 2016 年 11 月 10 日 17:20 UTC
- 編集日時: 2024 年 6 月 10 日 20:57 UTC
- ARN: arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v19 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",

```



```
"autoscaling:Describe*",
"aws-marketplace:ViewSubscriptions",
"backup:DescribeBackupJob",
"backup:DescribeBackupVault",
"backup:DescribeCopyJob",
"backup:DescribeFramework",
"backup:DescribeGlobalSettings",
"backup:DescribeProtectedResource",
"backup:DescribeRecoveryPoint",
"backup:DescribeRegionSettings",
"backup:DescribeReportJob",
"backup:DescribeReportPlan",
"backup:DescribeRestoreJob",
"backup:GetSupportedResourceTypes",
"backup:ListBackupJobs",
"backup:ListBackupPlanTemplates",
"backup:ListBackupPlanVersions",
"backup:ListBackupPlans",
"backup:ListBackupSelections",
"backup:ListBackupVaults",
"backup:ListCopyJobs",
"backup:ListFrameworks",
"backup:ListLegalHolds",
"backup:ListProtectedResources",
"backup:ListProtectedResourcesByBackupVault",
"backup:ListRecoveryPointsByBackupVault",
"backup:ListRecoveryPointsByLegalHold",
"backup:ListRecoveryPointsByResource",
"backup:ListReportJobs",
"backup:ListReportPlans",
"backup:ListRestoreJobs",
"backup:ListTags",
"batch:ListJobs",
"bedrock:ListCustomModels",
"bedrock:ListTagsForResource",
"clouddirectory:ListAppliedSchemaArns",
"clouddirectory:ListDevelopmentSchemaArns",
"clouddirectory:ListDirectories",
"clouddirectory:ListPublishedSchemaArns",
"cloudformation:DescribeStacks",
"cloudformation:List*",
"cloudfront:List*",
"cloudsearch:DescribeDomains",
"cloudsearch:List*",
```

```
"cloudtrail:DescribeTrails",
"cloudtrail:ListTrails",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"codebuild:ListBuilds*",
"codebuild:ListProjects",
"codecommit:List*",
"codedeploy:BatchGetApplicationRevisions",
"codedeploy:BatchGetApplications",
"codedeploy:BatchGetDeploymentGroups",
"codedeploy:BatchGetDeploymentInstances",
"codedeploy:BatchGetDeploymentTargets",
"codedeploy:BatchGetDeployments",
"codedeploy:BatchGetOnPremisesInstances",
"codedeploy:Get*",
"codedeploy:List*",
"codepipeline:ListPipelines",
"codestar:List*",
"cognito-identity:ListIdentities",
"cognito-identity:ListIdentityPools",
"cognito-idp:List*",
"cognito-sync:ListDatasets",
"comprehend:Describe*",
"comprehend:List*",
"config:Describe*",
"config:List*",
"connect:List*",
"cost-optimization-hub:GetPreferences",
"cost-optimization-hub:GetRecommendation",
"cost-optimization-hub:ListEnrollmentStatuses",
"cost-optimization-hub:ListRecommendationSummaries",
"cost-optimization-hub:ListRecommendations",
"databrew:ListJobs",
"databrew:ListProjects",
"datapipeline:DescribePipelines",
"datapipeline:GetAccountLimits",
"datapipeline:ListPipelines",
"dax:DescribeClusters",
"dax:DescribeDefaultParameters",
"dax:DescribeEvents",
"dax:DescribeParameterGroups",
"dax:DescribeParameters",
"dax:DescribeSubnetGroups",
```

```
"dax:ListTags",
"devicefarm:List*",
"directconnect:Describe*",
"discovery:List*",
"dms:List*",
"ds:DescribeDirectories",
"dynamodb:DescribeBackup",
"dynamodb:DescribeContinuousBackups",
"dynamodb:DescribeGlobalTable",
"dynamodb:DescribeGlobalTableSettings",
"dynamodb:DescribeLimits",
"dynamodb:DescribeReservedCapacity",
"dynamodb:DescribeReservedCapacityOfferings",
"dynamodb:DescribeStream",
"dynamodb:DescribeTable",
"dynamodb:DescribeTimeToLive",
"dynamodb:ListBackups",
"dynamodb:ListExports",
"dynamodb:ListGlobalTables",
"dynamodb:ListStreams",
"dynamodb:ListTables",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeBundleTasks",
"ec2:DescribeCarrierGateways",
"ec2:DescribeClassicLinkInstances",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeExportTasks",
"ec2:DescribeFlowLogs",
"ec2:DescribeHost*",
"ec2:DescribeIdFormat",
"ec2:DescribeIdentityIdFormat",
"ec2:DescribeImage*",
"ec2:DescribeImport*",
"ec2:DescribeInstance*",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
"ec2:DescribeLocalGatewayRouteTableVpcAssociations",
"ec2:DescribeLocalGatewayRouteTables",
```

```
"ec2:DescribeLocalGatewayVirtualInterfaceGroups",
"ec2:DescribeLocalGatewayVirtualInterfaces",
"ec2:DescribeLocalGateways",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeNetwork*",
"ec2:DescribePlacementGroups",
"ec2:DescribePrefixLists",
"ec2:DescribeRegions",
"ec2:DescribeReserved*",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshot*",
"ec2:DescribeSpot*",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolume*",
"ec2:DescribeVpc*",
"ec2:DescribeVpnGateways",
"ec2:SearchLocalGatewayRoutes",
"ecr:DescribeRegistry",
"ecr:DescribeRepositories",
"ecr:ListImages",
"ecs:Describe*",
"ecs:List*",
"eks:ListTagsForResource",
"elastic-inference:DescribeAcceleratorOfferings",
"elastic-inference:DescribeAcceleratorTypes",
"elastic-inference:DescribeAccelerators",
"elastic-inference:ListTagsForResource",
"elasticache:Describe*",
"elasticbeanstalk:DescribeApplicationVersions",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:DescribeEnvironments",
"elasticbeanstalk:ListAvailableSolutionStacks",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticmapreduce:List*",
"elastictranscoder:List*",
```

```
"emr-serverless:ListApplications",
"es:DescribeElasticsearchDomain",
"es:DescribeElasticsearchDomains",
"es:ListDomainNames",
"events:ListRuleNamesByTarget",
"events:ListRules",
"events:ListTargetsByRule",
"firehose:DescribeDeliveryStream",
"firehose:List*",
"fsx:DescribeFileSystems",
"gamelift:List*",
"glacier:List*",
"glue:GetTags",
"greengrass:List*",
"iam:GetAccountSummary",
"iam:GetLoginProfile",
"iam:List*",
"importexport:ListJobs",
"inspector:List*",
"iot:List*",
"kafka:ListClusters",
"kendra:ListDataSources",
"kendra:ListTagsForResource",
"kinesis:ListStreams",
"kinesisanalytics:ListApplications",
"kinesisanalytics:ListTagsForResource",
"kms:ListKeys",
"kms:ListResourceTags",
"lambda:List*",
"lex:GetBotAliases",
"lex:GetBotChannelAssociations",
"lex:GetBotVersions",
"lex:GetBots",
"lex:GetIntentVersions",
"lex:GetIntents",
"lex:GetSlotTypeVersions",
"lex:GetSlotTypes",
"lex:GetUtterancesView",
"lightsail:GetBlueprints",
"lightsail:GetBundles",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstances",
"lightsail:GetKeyPair",
"lightsail:GetRegions",
```

```
"lightsail:GetStaticIps",
"lightsail:IsVpcPeered",
"logs:Describe*",
"logs:ListTagsForResource",
"lookoutvision:ListModelPackagingJobs",
"lookoutvision:ListModels",
"lookoutvision:ListProjects",
"machinelearning:Describe*",
"mediaconnect:ListEntitlements",
"mediaconnect:ListFlows",
"mediaconnect:ListOfferings",
"mediaconnect:ListReservations",
"mobiletargeting:GetApplicationSettings",
"mobiletargeting:GetCampaigns",
"mobiletargeting:GetImportJobs",
"mobiletargeting:GetSegments",
"oam:ListAttachedLinks",
"oam:ListLinks",
"oam:ListSinks",
"opsworks-cm:Describe*",
"opsworks:Describe*",
"organizations:List*",
"outposts:GetOutpost",
"outposts:GetOutpostInstanceTypes",
"outposts:ListOutposts",
"outposts:ListSites",
"outposts:ListTagsForResource",
"polly:Describe*",
"polly:List*",
"profile:ListDomains",
"profile:ListIntegrations",
"rds:Describe*",
"redshift-serverless:ListTagsForResource",
"redshift-serverless:ListWorkgroups",
"redshift:DescribeClusters",
"redshift:DescribeEvents",
"redshift:ViewQueriesInConsole",
"resource-explorer-2:GetDefaultView",
"resource-explorer-2:GetIndex",
"resource-explorer-2:ListIndexes",
"resource-explorer-2:ListSupportedResourceTypes",
"resource-explorer-2:ListTagsForResource",
"resource-explorer-2:ListViews",
"route53:Get*",
```

```
"route53:List*",
"route53domains:List*",
"route53resolver:Get*",
"route53resolver:List*",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListMultiRegionAccessPoints",
"sagemaker:Describe*",
"sagemaker:List*",
"sdb:List*",
"servicecatalog:List*",
"ses:DescribeActiveReceiptRuleSet",
"ses:List*",
"ses:ListDedicatedIpPools",
"shield:List*",
"sns:List*",
"sqs:GetQueueAttributes",
"sqs:GetQueueUrl",
"sqs:ListDeadLetterSourceQueues",
"sqs:ListMessageMoveTasks",
"sqs:ListQueueTags",
"sqs:ListQueues",
"ssm:ListAssociations",
"ssm:ListDocuments",
"states:ListActivities",
"states:ListStateMachineAliases",
"states:ListStateMachineVersions",
"states:ListStateMachines",
"storagegateway:ListGateways",
"storagegateway:ListLocalDisks",
"storagegateway:ListVolumeRecoveryPoints",
"storagegateway:ListVolumes",
"swf:List*",
"trustedadvisor:Describe*",
"waf-regional:List*",
"waf:List*",
"wafv2:List*",
"workdocs:DescribeAvailableDirectories",
"workdocs:DescribeInstances",
"workmail:Describe*",
"workspaces:Describe*"
],
"Resource" : "*"
},
```

```
{
  "Effect" : "Allow",
  "Sid" : "APIGatewayAccess",
  "Action" : [
    "apigateway:GET"
  ],
  "Resource" : [
    "arn:aws:apigateway:*::/apis",
    "arn:aws:apigateway:*::/apis/*/authorizers/*",
    "arn:aws:apigateway:*::/apis/*/authorizers",
    "arn:aws:apigateway:*::/apis/*/cors",
    "arn:aws:apigateway:*::/apis/*/deployments/*",
    "arn:aws:apigateway:*::/apis/*/deployments",
    "arn:aws:apigateway:*::/apis/*/exports/*",
    "arn:aws:apigateway:*::/apis/*/integrations/*",
    "arn:aws:apigateway:*::/apis/*/integrations",
    "arn:aws:apigateway:*::/apis/*/models/*",
    "arn:aws:apigateway:*::/apis/*/models",
    "arn:aws:apigateway:*::/apis/*/routes/*",
    "arn:aws:apigateway:*::/apis/*/routes",
    "arn:aws:apigateway:*::/apis/*/stages",
    "arn:aws:apigateway:*::/apis/*/stages/*",
    "arn:aws:apigateway:*::/clientcertificates",
    "arn:aws:apigateway:*::/clientcertificates/*",
    "arn:aws:apigateway:*::/domainnames",
    "arn:aws:apigateway:*::/domainnames/*/apimappings",
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/authorizers/*",
    "arn:aws:apigateway:*::/restapis/*/authorizers",
    "arn:aws:apigateway:*::/restapis/*/deployments/*",
    "arn:aws:apigateway:*::/restapis/*/deployments",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/parts",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
    "arn:aws:apigateway:*::/restapis/*/documentation/versions",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
    "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
    "arn:aws:apigateway:*::/restapis/*/models/*",
    "arn:aws:apigateway:*::/restapis/*/models",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators",
    "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
    "arn:aws:apigateway:*::/restapis/*/resources/*",
    "arn:aws:apigateway:*::/restapis/*/resources",
    "arn:aws:apigateway:*::/restapis/*/stages",
```



```
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/tags/*",
    "arn:aws:apigateway:*::/vpclinks"
  ]
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

VMImportExportRoleForAWSConnector

説明： AWS コネクタを使用するお客様向けの VM Import/Export サービスロールのデフォルトポリシー。VM Import/Export サービスは、AWS コネクタ仮想アプライアンスからの仮想マシンの移行リクエストを実行するために、このポリシーを持つロールを引き受けます。(AWS コネクタは AWSConnector「」管理ポリシーを使用して、お客様に代わって VM Import/Export サービスにリクエストを発行することに注意してください。) AMIs と EBS スナップショットの作成、EBS スナップショット属性の変更、EC2 オブジェクトに対する「Describe*」呼び出し、import-to-ec「2-」で始まる S3 バケットからの読み取りを行う機能を提供します。

VMImportExportRoleForAWSConnector は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに VMImportExportRoleForAWSConnector をアタッチできます。

ポリシーの詳細

- タイプ: サービスロールポリシー
- 作成日時: 2015 年 9 月 3 日 20:48 UTC
- 編集日時: 2015 年 9 月 3 日 20:48 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

VPCLatticeFullAccess

説明： Amazon VPC Lattice へのフルアクセスと依存関係サービスへのアクセスを提供します。

VPCLatticeFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 30 日 02:49 UTC
- 編集日時: 2023 年 3 月 30 日 02:49 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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"
  }
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

VPCLatticeReadOnlyAccess

説明： 経由で Amazon VPC Lattice への読み取り専用アクセスと AWS Management Console、依存関係サービスへの制限付きアクセスを提供します。

VPCLatticeReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2023 年 3 月 30 日 02:47 UTC
- 編集日時: 2023 年 3 月 30 日 02:47 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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" : "*"
}
]
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

VPCLatticeServicesInvokeAccess

説明： Amazon VPC Lattice サービスを呼び出すためのアクセスを提供します。

VPCLatticeServicesInvokeAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに VPCLatticeServicesInvokeAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー

- 作成日時: 2023 年 3 月 30 日 02:45 UTC
- 編集日時: 2023 年 3 月 30 日 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーの使用を開始し、最小特権のアクセス許可に移行する](#)

WAFLoggingServiceRolePolicy

説明: 顧客のログを Firehose ストリームに書き込む SLR の作成

WAFLoggingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 21:05 UTC
- 編集日時: 2018 年 8 月 24 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

```
}
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

WAFRegionalLoggingServiceRolePolicy

説明：顧客のログを Firehose ストリームに書き込む SLR の作成

WAFRegionalLoggingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2018 年 8 月 24 日 18:40 UTC
- 編集日時: 2018 年 8 月 24 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "firehose:PutRecord",
      "firehose:PutRecordBatch"
    ],
    "Resource" : [
      "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
    ]
  }
]
```

詳細はこちら

- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

WAFV2LoggingServiceRolePolicy

説明：このポリシーは、AWS WAF が Amazon Kinesis Data Firehose にログを書き込むことを許可するサービスにリンクされたロールを作成します。

WAFV2LoggingServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

ポリシーの詳細

- タイプ: サービスリンクロールポリシー
- 作成日時: 2019 年 11 月 7 日 00:40 UTC
- 編集日時: 2024 年 6 月 3 日 17:29 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

ポリシーのバージョン

ポリシーのバージョン: v3 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM ポリシーのバージョンニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

WellArchitectedConsoleFullAccess

説明： 経由で AWS Well-Architected Tool へのフルアクセスを提供します AWS Management Console

WellArchitectedConsoleFullAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに WellArchitectedConsoleFullAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 18:19 UTC
- 編集日時: 2018 年 11 月 29 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

WellArchitectedConsoleReadOnlyAccess

説明： 経由で AWS Well-Architected Tool への読み取り専用アクセスを提供します AWS Management Console

WellArchitectedConsoleReadOnlyAccess は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに WellArchitectedConsoleReadOnlyAccess をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2018 年 11 月 29 日 18:21 UTC
- 編集日時: 2023 年 6 月 29 日 17:16 UTC
- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess

ポリシーのバージョン

ポリシーのバージョン: v2 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)
- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

WorkLinkServiceRolePolicy

説明： Amazon が使用または管理する AWS のサービス およびリソースへのアクセスを有効にします WorkLink

WorkLinkServiceRolePolicy は [AWS マネージドポリシー](#) です。

このポリシーを使用すると

ユーザー、グループおよびロールに WorkLinkServiceRolePolicy をアタッチできます。

ポリシーの詳細

- タイプ: AWS 管理ポリシー
- 作成日時: 2019 年 1 月 23 日 19:03 UTC

- 編集日時: 2019 年 1 月 23 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

ポリシーのバージョン

ポリシーのバージョン: v1 (デフォルト)

ポリシーのデフォルトバージョンは、ポリシーのアクセス許可を定義するバージョンです。ポリシーを持つユーザーまたはロールが AWS リソースへのアクセスをリクエストすると、はポリシーのデフォルトバージョン AWS をチェックして、リクエストを許可するかどうかを判断します。

JSON ポリシードキュメント

```
{
  "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-*"
    }
  ]
}
```

詳細はこちら

- [IAM Identity Center で AWS マネージドポリシーを使用してアクセス許可セットを作成する](#)

- [IAM ID のアクセス許可の追加および削除](#)
- [IAM ポリシーのバージョニングについて理解する](#)
- [AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する](#)

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。